© dTosh | stock.adobe.com

Making Warrants Great Again:

Avoiding General Searches in the Execution of Warrants for Electronic Data

I. Introduction

Today, a massive amount of revealing, personal information is stored on computers and cellphones, and "in the cloud" — internet-connected servers hosted by the scores of online companies whose products and services people use on a daily basis. Carrying a cellphone, using social media, or taking advantage of online services generates a vast quantity of sensitive and private information. Law enforcement can obtain this information from phones and computers, or from the online entities that gather, store, analyze, and sometimes sell people's confidential histories.

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 cellphone, track someone's physical location, or obtain vast, sensitive, and revealing records about people from service providers.[1] These recent precedents are vital. But the question of whether a warrant is required is only the first critical step. The next question, of equal importance, is "what does a warrant require?" For the warrant requirement to protect civil liberties and privacy, warrant protections must be robust.

Current search warrant practice falls short in a number of ways. The first is *lack of nexus*: Courts will find probable cause on the mere basis that people, including criminals, frequently use electronic devices and online accounts, so evidence must be likely to be found there. Second is *overseizure*: Many warrants seek to seize and/or search "all content," "all data," or a laundry list of data types meant to capture everything, even though evidence is unlikely to exist in that form or to have been generated during that time frame. And third, *rummaging searches*: Some courts have been extremely permissive, largely accepting government claims that once investigators seize data, they may examine files in a discretionary and happenstance manner because relevant evidence could be found anywhere.

The ACLU recently has filed a number of amicus briefs in state and federal courts challenging these practices. This article complements those briefs and lays out the legal arguments in favor of a nexus requirement and narrow, tailored searches and seizures. A longer version of this discussion appears on the ACLU website. That paper additionally addresses data retention and the reasonable expectation of privacy, and it includes an appendix containing copies of the ACLU's briefing in this area.[2]

Unfortunately, the good faith exception to the exclusionary rule poses a serious obstacle to obtaining relief for searches or seizures that violate the Constitution. Generally, defendants must show that "the warrant is based on an affidavit so lacking in probable cause as to render

BY JENNIFER S. GRANICK

belief in its existence unreasonable" or that "the warrant is facially deficient in particularizing the place to be searched or things to be seized."[3] This is particularly hard when the case law develops so slowly, ironically because courts refuse to decide the substantive Fourth Amendment questions in favor of disposing of the case on good-faith grounds.[4] Nevertheless, there is strong precedent that courts should decide the substantive issue first, and doing so will help future defendants who can point to that ruling as evidence that the police officers' faith in an inadequate warrant was unjustified.[5]

II. Electronic data search warrants can look a lot like general warrants.

Private digital data is voluminous and extremely sensitive.[6] Online accounts are especially extensive.[7] These data repositories include 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. They 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.

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.[8] Nor can they rummage through a medicine cabinet to look for a flat-screen television.[9]

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. An affidavit in support of a warrant to search a hard drive or online account may demonstrate probable cause that, among these most sensitive files, there is likely evidence of a crime. But innocent information and potential evidence are not easily disentangled. Because of the inherently intermingled nature of electronic data, in most instances the government will overseize information and sort through it later. This means that police are routinely seizing and searching information for which they do not have probable cause. This is a situation ripe for unconstitutional general invasions of privacy and for police to concoct theories of guilt adorned with whatever photos, suggestive text messages, or other information they find.

Many people other than the target will be swept up in such sweeping investigations. 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). Overbroad digital searches and seizures, far more than physical-world investigations, invade the privacy of scores of people who are not suspects. While defendants generally must prove that their own expectation of privacy was invaded, the fact that scores of other people were also swept into the law enforcement dragnet is compelling evidence that a warrant was overbroad.[10]

III. Warrants must robustly adhere to the Fourth Amendment's particularity and probable cause requirements to avoid being unconstitutional.

While the Supreme Court has held that "digital" is different,[11] even traditional Fourth Amendment doctrine supports the argument for especially robust, narrowly tailored search warrants for electronic information.

Warrants are intended to prevent general searches,[12] and to avoid a "general, exploratory rummaging in a person's belongings."[13] An affidavit supporting a search warrant must indicate "that contraband or evidence of a crime will be found in a particular place."[14] There must "be a nexus … between the item to be seized and criminal behavior."[15]

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. Opposition to general warrants, which 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," was "one of the driving forces behind the Revolution itself."[16]

Warrants must also *particularly describe* the things to be searched and seized. They must serve as a practical guide for officers. The amount of specificity required is necessarily flexible, but particularity depends on case-specific facts: the type of crime, the facts already known by the officers, the facts that should be known by the officers, and other considerations on a case-by-case basis.[17]

These longstanding principles are especially salient in the digital context: 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."[18]

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.

IV. A warrant affidavit must establish a factual nexus between electronically stored data and the investigation.

Data seizures must be supported by probable cause. However, 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.[19] The affidavits commonly lack case-specific reasons to believe that evidence of the crime under investigation will be found on the particular devices or services. A court then improperly issues a warrant. But 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.[20]

An officer's training and experience can often be a basis for probable cause, but there still 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. 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. In *United States v. Brown*, the Sixth Circuit suppressed evidence obtained pursuant to a warrant because the affidavit in support of the warrant request "failed to establish the required nexus between the alleged drug trafficking and Brown's residence."[21] There must be some reliable evidence connecting the known drug dealer's ongoing criminal activity to the residence, such as an informant who observed drug deals or drug paraphernalia in or around the residence.[22] Similarly, the averment that a defendant is allegedly in a gang should not alone be sufficient for probable cause.[23]

Current search warrant practice falls short in three ways: lack of nexus, overseizure, and rummaging searches.

In *Commonwealth v. Broom*, the affiant asserted that in his training and experience "cellular telephones contain multiple modes used to store vast amount of electronic data;" and that many types of data the detective sought to examine would be found on the defendant's cellular telephone.[24] But without "a substantial, particularized basis reasonably to expect that the files on the cellular telephone that police sought to search would contain information related to the homicide under investigation," especially because other information suggested that the victim and the suspect had not communicated by phone that evening, the Massachusetts Supreme Judicial Court held that the warrant was "general" and "conclusory" and not supported by probable cause.[25]

In *Commonwealth v. White*, the Massachusetts high 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.[26] 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.[27]

The Texas Court of Criminal Appeals in *State v. Baldwin* made the same point in holding that a warrant to search a phone was insufficient.[28] Boilerplate language asserting that it is common for criminals to store evidence on phones must be accompanied by additional facts. In *Baldwin*, the "'other fact' … that two Black men committed the offense together" was insufficient to connect the mobile phone to the offense.[29]

It is a slippery slope when courts automatically find probable cause to search electronic devices. Therefore, 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.

V. Warrants may not authorize seizure of all data, but they should be limited by category of data, date range, and other filters to the extent possible.[30]

With cellphones and laptops, if computer hardware is contraband, an instrumentality of a crime, or the fruits of a crime, investigators may physically seize it.[31] But even when the seizure is based on the likelihood that evidence may be stored on hard drives or mobile phones, courts have generally been convinced that seizure of the entire device and all data on it is necessary to (1) create a forensically sound mirror or image copy; and (2) to conduct a proper investigative search because investigators cannot meaningfully segregate responsive from non-responsive data on site. Thus, courts have generally authorized broad seizures of stored data for logistical reasons, justified by constraints at the search stage.[32] Rule 41 of the Federal Rules of Criminal Procedure expressly contemplates the need for this two-stage process.[33]

Yet *seize first, search second* is not always constitutional. Any overseizure must still be "reasonable" within the meaning of the Fourth Amendment. Rule 41 does not (and constitutionally could not) authorize seizures of data that are unnecessary or unreasonable in the context of a particular investigation.[34]

Whatever the merits of a *seize first, search second* approach in the context of computer hard drives, the same considerations do not justify seizures of data in an email or social media account. Courts may not issue warrants purporting to authorize seizure of all data from an electronic account (all-data or all-content warrants).[35]

First, providers can preserve 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. Second, the service provider generally has the capability to filter out irrelevant categories of data or irrelevant time frames.[36]

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.[37] 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."[38] 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.[39]

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

A. Warrants must limit the categories of data to be seized from social media or cloud-storage accounts to those responsive to probable cause.

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 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.[40] These warrants are susceptible to attack. With respect to data in online accounts, a provider may be capable of initially sorting some non-

responsive information out of the trove provided to law enforcement. A search warrant to Facebook demanding all of a 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 is likely overbroad.[41] If, for example, a case involves a conspiracy to sell drugs, the police do not need passwords, tagged posts, or "likes." 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.'"[42]

Defense attorneys have strong grounds to challenge "all-data," "all-content," or boilerplate warrants containing comprehensive lists of types of data on overbreadth grounds — warrants to online service providers should list only relevant categories of data tailored to the investigation at hand.

B. Warrants without a date range are also overbroad.

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.

For seizures of data from online service providers, it will almost always be feasible to request materials from a limited date range.[43] For example, in *In re Search of Information Associated with Four Redacted Gmail Accounts*, the warrant sought all emails associated with the suspect's account.[44] 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*, the Oregon Supreme Court held that the warrant to search the defendant's computer was proper because it was limited to search history on the day of a child's injury and death.[45] The state's subsequent search, through data from weeks and months before the death, was outside the scope of the warrant, and impermissible.[46] Similarly, in *Commonwealth v. Snow*, the Massachusetts Supreme Judicial Court found that a warrant to search the cellphone 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.'"[47]

Warrants may also be overbroad because the seized data could have easily been narrowed further based on case-specific filters. For example, officers could easily limit an email warrant to demand only messages between co-conspirators. Parsing messages between specific users is a commonplace functionality, just as account holders search their own inboxes. The government may also have had an obligation to limit its acquisition to mail sent by the suspect, rather than from unrelated third parties, or exclude emails between suspects and their attorneys, clergy, doctors, or spouses. Several magistrate judges have refused to issue warrants without such filtering by keyword, communicants, or other factors, though frequently the district court has overruled them.[48]

Images may be another area in which providers' built-in search capabilities enable more tailored data seizures.[49] Investigators might seek from a service like Google Photos only those images that were taken at a particular location or that contain the face of a particular person of interest.

The government's 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. All true. 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 investigatory expertise to perform. Investigators can then follow up on any leads by obtaining a second warrant.

VI. Warrants must cabin data searches to probable cause.

The same principle applies to searches just as well as seizures. Investigators should not be permitted to rummage through cellphones or social media accounts, as this practice exposes swaths of private information for which there is no probable cause to the government. Especially when logistical necessities justify the government's overbroad data seizures, courts must be vigilant in ensuring that any subsequent search is sufficiently narrow.

The Ninth Circuit has issued an in-depth decision discussing the problem of restraining searches of intermingled evidence. In *Comprehensive Drug Testing, Inc.*, law enforcement officers obtained a warrant to search the electronically stored drug-testing records of 10 Major League Baseball players.[50] 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 10 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.[51] The Ninth Circuit did not *impose* these limitations on future searches, however.

The *CDT* analysis remains important and influential, but it leaves open many questions.[52] Are the listed safeguards required by the Fourth Amendment? Do judges have the authority to impose these restrictions?[53] 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 scoped search turns up evidence of a new offense?

Ultimately, *CDT* assumes that broad seizures and broad searches are reasonable, and looks for ways to ensure that investigators do not get a windfall of evidence unrelated to probable cause. However, broad seizures and broad searches will often be outside the scope of probable cause *and unnecessary*. The first step to protecting Fourth Amendment interests is to limit the amount of non-responsive data that may be accessed by law enforcement in the first instance. The second step is for the warrant to limit searches of that data.

A. Warrants may not authorize searches of all content, and should be limited by date range and category, among other parameters.

Frequently, warrants state that officers may search "all content" on a device, or a comprehensive laundry list of files and folders, for evidence. This authorization may be limited by the requirement that the search be for evidence of the crime for which there is probable cause. The warrant does not contain other parameters for the search. The presumption is that officers must have the discretion to review all the data on the grounds that evidence could be hidden anywhere.[54]

In fact, it is not as easy to hide data as the government frequently asserts. As explored in the *Shipp* case, social media and other online data is classified by the provider and there is no way to, for example, hide an incriminating photo in a rejected friend request.[55] And for cellphones, data is generally not stored according to the user's wishes, but as designed by the operating system manufacturer. As the tech policy nonprofit Upturn explained in an amicus brief filed in the case *State v. Smith*, modern cellphones operate differently from computers "because mobile operatizing systems are designed for ease of use and do not emphasize user-directed file organization."[56] "As any iPhone or Android user can tell, users no longer determine where an app stores its files, because users have no direct access to the file directory."[57] "This layer of abstraction over the cellphone's core functions (that computers do not exhibit to the same extent) means that cellphone users are generally not able to directly manipulate their cellphone data."[58]

Furthermore, today's forensic tools are powerful enough to find images and documents regardless of file names, file extensions, or where they are stored. For example, forensic tools can still discover and display an image file hidden in an unexpected folder and renamed with a misleading file extension.[59] Moreover, the rare occasion where a user is especially sophisticated should not justify a default rule for broad searches of most cellphones.

Were courts to adopt the argument that police can look at all the information they seize, there would be no meaningful limit to searches or seizures of digital information. For this reason, the Michigan Supreme Court rejected the state's argument that an officer may always review all digital data seized pursuant to a warrant on the basis of the possibility that evidence may be concealed, mislabeled, or manipulated. "Such a *per se* rule would effectively nullify the particularity requirement of the Fourth Amendment in the context of cellphone 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.'"[60]

An increasing number of courts, therefore, are holding that searching in the right place, not *every* place, is the only plan that complies with the Constitution.[61] For example, probable cause to search for photographs does not amount to probable cause to search for web history.[62] And probable cause to determine whether a suspect's phone had a flashlight function does not authorize general rummaging through the phone's entire contents.[63]

Warrants can limit searches for electronic evidence by file type as well as by description and time without unduly interfering with law enforcement investigations. If there is probable cause to believe that co-conspirators texted each other, there is no reason in the first instance to search photos. If investigators learn that suspicious texts attach photos, then the search can expand to those (and related) photos, either pursuant to a sec-

ond warrant or under the first warrant as overseen by the issuing judge. U.S. Supreme Court precedent supports limiting searches by file type or category. *Riley* explicitly discussed the invasiveness of law enforcement access to different "categories," "areas," "types" of data, and "apps."[64] The Court also pointed out that "certain types of data are qualitatively different" from others in terms of privacy.[65]

For example, 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 constitution's particularity requirements.[66] 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 emphasized that more specificity is required than simply identifying the smartphones to be searched and allowing a search of all data "pertinent to the criminal investigation."[67] Of course, not all courts have taken this approach yet.[68]

Warrants can limit searches based on time frame, information sought, *and* file type — especially when authorizing searches of sensitive categories of data such as personal conversations. For example, in *People v. Herrera*, the Colorado Supreme Court suppressed evidence contained in a text message involving a third party not named in the warrant. The court held that the government's argument that *any* text message folder could be searched because of the abstract possibility that the folder might contain indicia of who owned the phone, or might have been deceptively labeled, would result in an unconstitutional limitless search.[69] Thus, the appropriate search criteria would have identified the relevant file type (text messages) *and* the text conversations relevant to the inquiry (those involving the individuals named in the warrant). These functional limitations can be constitutionally required, as the law is clear that police cannot get a warrant to seize or search categories of data for which there is no probable cause.

In a similar vein, when a search is authorized by consent rather than by a warrant, the search must not exceed the scope of that consent.[70] All government inspections must be tied to the underlying authority for that search.

Courts should be especially receptive to this argument because examining everything, even cursorily, is impossible. There is no way that investigators tasked with making sense of a flood of data, the vast majority of which has nothing to do with criminal activity, can do so without targeted searches. The officers will inevitably be exercising their discretion, and the Fourth Amendment is clear that their discretion must be cabined by the warrant.[71] These limitations are needed to prevent "general rummaging" when searching electronically stored information such as email accounts.[72]

B. 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, in several recent cases the government raised a host of reasons 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.

In *United States v Carey*, 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).[73] 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. 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.[74]

In contrast, in *United States v. Walser*, 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."[75] 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.[76]

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. For example, the Michigan Supreme Court, in *People v. Hughes*, rejected the state's view that once a warrant issues to search a cellphone for evidence of one crime, the defendant no longer has a reasonable expectation of privacy in any of his data. The court held that a seizure deprives an individual of control over the property but does not reduce his reasonable expectation of privacy in the contents of the property.[77] 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.[78]

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.[79] In *United States v. 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.[80] 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.[81] 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.

While courts are increasingly accepting this conclusion, there are as yet no answers to how long police may retain data. At a certain point — two-and-a-half years in *Ganias* — 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 overly long data retention, and without the data, the warrant would be pointless.[82]

VII. Conclusion

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. 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. Proper use of forensic tools could further limit exposure of private information to police officers and also enable judicial oversight of searches. Rather than defer to agents' judgment, courts must use the tools at their disposal to ensure this outcome. Data should be segregated and the non-responsive data should be sequestered and ultimately returned or deleted.

While it is challenging to obtain suppression for an individual client, litigating these issues can improve outcomes and dissuade privacy violations overall.

Notes

1. *See* Riley v. California, 573 U.S. 373 (2014); United States v. Jones, 565 U.S. 400 (2012); Carpenter v. United States, 138 S. Ct. 2206 (2018).

2. ACLU, *The Warrant Clause in the Digital Age* (Dec. 2021), https://www.aclu.org/warrant-clause-digital-age.

3. United States v. Leon, 468 U.S. 897, 923 (1984).

4. *See, e.g.*, United States v. Moore, 968 F.2d 216, 222 (2d Cir. 1992).

5. United States v. Dahlman, 13 F.3d 1391, 1397 (10th Cir. 1993) (quoting *Leon*, 468 U.S. at 924–925) (courts should address Fourth Amendment issues before turning to good faith unless there is no danger of "freezing" Fourth Amendment jurisprudence).

6. *See* United States v. Payton, 573 F.3d 859, 861–62 (9th Cir. 2009).

7. *See, e.g.*, GOOGLE, *About Google One*, https://one.google.com/about (last visited Oct. 14, 2022) (Google offers 15 gigabytes of data storage for free, and up to two terabytes (2,000 gigabytes) of storage at negligible cost).

8. *See, e.g.*, Horton v. California, 496 U.S. 128, 141 (1990).

9. *See, e.g.*, United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013).

10. In re Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that Is Stored at Premises Controlled by Facebook, Inc. (*Aaron.Alexis*), 21 F. Supp. 3d 1, 7 (D.D.C. 2013) (no probable cause existed for obtaining information about all people who communicated with the user, or members of shared Facebook groups).

11. *Riley*, 573 U.S. 373.

12. Groh v. Ramirez, 540 U.S. 551, 561 (2004).

13. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

14. Illinois v. Gates, 462 U.S. 213, 238 (1983).

15. Warden, Md. Penitentiary v. Hayden, 387 US 294, 307 (1967); *accord* United States v. Brown, 828 F.3d 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).

16. Steagald v. United States, 451 U.S. 204, 220 (1981); *Riley*, 573 U.S. at 403.

17. *See Galpin*, 720 F.3d at 446; 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)).

18. United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (collecting cases); *Galpin*, 720 F.3d at 447; *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.").

19. *See, e.g.*, People v. Hughes, 958 N.W.2d 98, 110 n.6 (Mich. 2020) (court did not decide whether, in drug trafficking investigation, affidavit filed in support of warrant to search the defendant's cellphone 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) (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 cellphones nor using a cellphone just prior to or during arrest would, in the absence of other evidence, provide probable cause); *Brown*, 828 F.3d at 384 ("[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 Cir. 2019) (cellphones 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); United States v. Garay, 938 F.3d 1108, 1113 (9th Cir. 2019) (Probable cause was found in a 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 cellphones inside car, and affidavit stating that in officers' experience people who possess firearms "like to take pictures of [those items]" with their cellphones, and "will also communicate via text" regarding criminal activity.).

20. The appendix accompanying the *Making Warrants Great Again* whitepaper contains ACLU briefs challenging search warrants on the grounds of lack of nexus. *See* Jennifer S. Granick, ACLU, *Making Warrants Great Again* (Dec. 2021), available at https://www.aclu.org/sites/default/files/field_document/mwga_appx_appx_table.pdf.

21. *Brown*, 828 F.3d at 385.

22. *Id*. at 383.

23. State v. Keodara, 364 P.3d 777, 782 (Wash. Ct. App. 2015), *review denied*, 377 P.3d 718 (Wash. 2016) (blanket statements about what certain groups of offenders tend to do and what information they tend to store in particular places, without evidence of the use of defendant's phone to commit any illicit activity, is insufficient under the Fourth Amendment).

24. Commonwealth v. Broom, 52 N.E.3d 81, 89 (Mass. 2016).

25. *Keodara*, 364 P.3d at 783 (affidavit that officers' training and experience was that gang members commonly take photographs of themselves holding guns insufficient to establish probable cause); *see also* State v. Castagnola, 46 N.E.3d 638, 657–61 (2015) (defendant's statement that he had to "look up" victim's address insufficient to establish probable cause to search computer).

26. Commonwealth v. White, 59 N.E.3d 369 (Mass. 2016).

27. *Id.* at 377 (quoting *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 cellphone.'").

28. State v. Baldwin, No. PD-0027-21, 2022 WL 1499508 (Tex. Ct. Crim. App. May 11, 2022).

29. *Id.* at *11.

30. The Fourth Amendment requires similar targeting in conducting the search, discussed later in this article.

31. Fed. R. Crim. P. 41.

32. Search Warrant to Sony Interactive at 6–8, In re Search of Info. Associated with the Electronic Account for PlayStation User "Speedola20," No. 4:19-SW-00364-JTM (W.D. Mo. Oct. 22, 2019) (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.

33. *See* Fed. R. Crim. P. 41(e)(2)(b).

34. United States v. Hill, 459 F.3d 966, 974–75 (9th Cir. 2006) (government must demonstrate to magistrate why broad search and seizure authority is reasonable in the case at hand).

35. *See* United States v. Blake, 868 F.3d 960, 966–67 (11th Cir.), *cert. denied*, 138 S. Ct. 753 (2017) (probable cause to search the Facebook account but the search warrant 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. Aug. 30, 2019) (probable cause showed that suspects communicated over Facebook 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 "check ins" were overbroad).

36. *See, e.g.*, *Snow*, 160 N.E.3d at 286–87, 289 (search warrant allowed officers to search virtually every area on the cellphone, court held that suppression may be required because search warrant did not specify date parameters).

37. *Blake*, 868 F.3d at 974 (11th Cir. 2017).

38. United States v. Shipp, 392 F. Supp. 3d 300, 303–06 (E.D.N.Y. 2019).

39. 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). 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.

40. In re Application of the U.S. for an Order Authorizing Disclosure of Historical Cell Site Info. for Tel. No. [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."); *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"].

41. United States v. Shipp, 392 F. Supp. 3d 300, 303–06 (E.D.N.Y. 2019).

42. *Id.* (citing United States v. Ross, 456 U.S. 798, 824 (1982)).

43. *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.") (citation omitted); United States v. Diaz, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure records dated 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).

44. In re Search of Info. Associated with Four Redacted Gmail Accounts, 371 F. Supp. 3d 843, 844 (D. Or. 2018).

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

46. *Id.* at 343–44 (interpreting Article I, section 9 of the Oregon Constitution).

47. Commonwealth v. Snow, 160 N.E.3d 277, 282 (Mass. 2021); *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).

48. In re 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), *objections sustained in part and overruled in part by* In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp., 212 F. Supp. 3d 1023, 1037 (D. Kan. September 28, 2016); *see also* In re the Search of Info.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), *order vacated by* In re Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157 (D.D.C. 2014); In the Matter of Applications for Search Warrants for Info.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).

49. *See, e.g.*, Google, *About Google Photos*, https://www.google.com/photos/about/ (last visited Oct. 14, 2022) (explaining that photos saved to Google photos "are organized and searchable by the places and things in them — no tagging required").

50. United States v. Comprehensive Drug Testing (*CDT*), 621 F.3d 1162, 1176 (9th

Cir. 2010) (en banc) (per curiam), *overruled in part on other grounds as recognized by* Demaree v. Pederson, 877 F.3d 870, 876 (9th Cir. 2018) (per curiam).

51. *CDT* recommended that magistrate judges insist that the government forswear reliance on the plain view doctrine; 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; and fairly disclose the actual degree of risk of concealment or destruction of evidence in the case at hand. Also, 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, and require an independent search team, especially in cases where the party subject to the warrant is not suspected of any crime. Finally, the government must destroy or return non-responsive data. 621 F.3d at 1180.

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

53. *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).

54. United States v. Williams, 592 F.3d 511, 519–20 (4th Cir. 2010) (as 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; *but see* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (officers must conduct search in a way that avoids searching files of types not identified in the warrant).

55. *Shipp*, 392 F. Supp. 3d at 303-06.

56. Amicus Curiae Brief of Upturn Inc., in Support of Defendant-Appellant, S.C. 20600, *citing* Andrew D. Huynh, *What Comes After Get a Warrant: Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 CORNELL L. REV. 187, 207-208 (2015).

57. *Id*. (citing Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 IOWA L. REV. 1643, 1660 (2020)).

58. *Id.*

59. Logan Koepke et al., MASS EXTRACTION: THE WIDESPREAD POWER OF U.S. LAW ENFORCEMENT TO SEARCH MOBILE PHONES, UPTURN (Oct. 2020).

60. People v. Hughes, 958 N.W.2d 98, 117–118 (Mich. 2020) (quoting *Riley*, 573 U.S. at 399).

61. *See, e.g.*, Burns v. United States, 235 A.3d 758, 775 (D.C. 2020) (warrant authorizing search of everything on phone when affidavits established probable cause only for three narrow categories was "constitutionally intolerable"); State v. Henderson, 854 N.W.2d 616 (Neb. 2014) (warrants permitting a search of "[a]ny and all information" did not comply with the particularity requirement, even though warrant listed the crimes under investigation); *see also* In re U.S. Application for a Search Warrant to Seize & Search Elec. 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).

62. 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).

63. State v. McLawhorn, 2020 WL 6142866, *24–*26 (Tenn. Ct. 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 cellphone 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).

64. *Riley*, 573 U.S. at 395, 396, 399.

65. *Id.*

66. Taylor v. State, 260 A.3d 602 (Del. 2021).

67. *Id*. at 616.

68. Commonwealth v. Green, 265 A.3d 541 (Pa. 2021) (search warrant was not overbroad due to the failure to include specific dates, types of files, or specific programs).

69. People v. Herrera, 357 P.3d 1227, 1230, 1233–34 (Colo. 2015).

70. State v. Mefford, No. DA 20-0330, 2022 WL 4480816 (Mont. Sept. 27, 2022).

71. United States v. Zemlyansky, 945 F. Supp. 2d 438, 459 (S.D.N.Y. 2013) (internal quotation marks, citations, 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").

72. *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").

73. United States v. Carey, 172 F.3d 1268, 1270–71 (10th Cir. 1999).

74. *Id*. at 1276.

75. United States v. Walser, 275 F3d 981, 984–85 (10th Cir. 2001).

76. *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).

77. *Hughes*, 958 N.W.2d at 111, 14–15.

78. *See also* People v. McCavitt, 185 N.E.3d 1192, 1206–07 (Ill. 2021) (owner retains expectation of privacy in forensic copy of hard drive data).

79. *See* United States v. Ganias (*Ganias I*), 755 F.3d 125 (2d Cir. 2014), *rev'd en banc on other grounds by* 824 F.3d 199 (2d Cir. 2016) (*Ganias II*).

80. *Ganias I*, 755 F.3d at 137.

81. *Ganias II*, 824 F.3d at 209.

82. *See Hughes*, 958 N.W.2d 98; State v. Burch, 961 N.W.2d 314 (Wisc. 2021); and *McCavitt*, 185 N.E.3d 1192. ■

About the Author

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.

Jennifer Granick
American Civil Liberties Union
San Francisco, California
415-343-0758
EMAIL jgranick@aclu.org