No. 23-469

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff-Appellee,

v.

JOHN HOLCOMB

Defendant-Appellant.

On Appeal from the United States District Court
for the Western District of Washington at Seattle

No. CR21–75–RSL
Hon. Robert S. Lasnik

BRIEF FOR AMERICAN CIVIL LIBERTIES UNION & AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION AS *AMICI CURIAE* SUPPORTING DEFENDANT-APPELLANT JOHN HOLCOMB

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION

Jazmyn Clark
P.O. Box 2728
Seattle, WA 98111
Tel: (206) 624-2184
E-mail: jclark@aclu-wa.org

AMERICAN CIVIL LIBERTIES UNION FOUNDATION

Jennifer Stisa Granick
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
E-mail: jgranick@aclu.org

Brett Max Kaufman
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
E-mail: bkaufman@aclu.org

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, *amici curiae* state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

DATED this November 20, 2023

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES iv

STATEMENT OF INTEREST OF *AMICI CURIAE* 1

INTRODUCTION & SUMMARY OF ARGUMENT 2

FACTS 3

ARGUMENT 6

I. Longstanding Fourth Amendment rules prohibit free-ranging searches, including searches of digital information. 6

A. The Fourth Amendment has long required that warrants clearly limit what officers may seize and police searches must be designed to find relevant information the seizure of which is supported by probable cause. 6

B. Computers and other digital devices contain an immense amount of private, sensitive data. 9

C. The overbreadth and particularity provisions of the Fourth Amendment are especially important when officers search electronic information. 11

II. Traditional Fourth Amendment principles make clear that probable cause to search or seize some data on a digital device does not justify access to the totality of the device's contents. 13

III. Warrants must ensure that overseizures of data are not exploited in ways that give law enforcement a windfall simply because potential evidence is digital in nature. 19

A. Courts should limit searches by time frame to ensure they do not expand beyond data relevant to the crime under investigation. 19

B. Courts should limit searches by file type to ensure they do not expand beyond data relevant to the crime under investigation. 20

C. Forensic tools make it straightforward for law enforcement to narrow searches by file type, date range, and other limitations that adhere closely to probable cause. 21

IV. Officers should have known that the search that turned up the relevant evidence in this case violated the Fourth Amendment, and the good faith exception should not apply. 25

CONCLUSION 27
CERTIFICATE OF SERVICE 29

TABLE OF AUTHORITIES

Cases

Arizona v. Gant,
556 U.S. 332 (2009) 7

Berger v. New York,
388 U.S. 41 (1967) 7, 12

Burns v. United States,
235 A.3d 758 (D.C. 2020) 14

Carpenter v. United States,
138 S. Ct. 2206 (2018) 1, 7, 10, 13

Carroll v. United States,
267 U.S. 132 (1925) 13

Ferguson v. City of Charleston,
532 U.S. 67 (2001) 10

Florida v. Harris,
568 U.S. 237 (2013) 7

Groh v. Ramirez,
540 U.S. 551 (2004) 7

Horton v. California,
496 U.S. 128 (1990) 11

In re [REDACTED]@gmail.com,
62 F. Supp. 3d 1100 (N.D. Cal. 2014) 20

In re Search of Google Email Accounts identified in Attachment A,
92 F. Supp. 3d 944 (D. Alaska 2015) 20

In re U.S. Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius,
770 F. Supp. 2d 1138 (W.D. Wash. 2011) 18

Kentucky v. King,
563 U.S. 452 (2011) 7

Kyllo v. United States,
533 U.S. 27 (2001) 13

Maryland v. Garrison,
480 U.S. 79 (1987) 8

People v. Frank,
700 P.2d 415 (Cal. 1985) 8

People v. Hughes,
958 N.W.2d 98 (Mich. 2020) 14

Riley v. California,
573 U.S. 373 (2014) 9, 10, 11, 14

Stanford v. Texas,
379 U.S. 476 (1965) 6, 7

State v. Bock,
485 P.3d 931 (Or. Ct. App. 2021) 18

State v. Mansor,
421 P.3d 323 (Or. 2018) 15

State v. McLawhorn,
636 S.W.3d 210 (Tenn. Crim. App. 2020) 16

State v. Missak,
299 A.3d 821 (N.J. Super. Ct. App. Div. 2023) 16, 24, 25

State v. Wilson,
884 S.E.2d 298 (Ga. 2023) 15, 27

Taylor v. State,
260 A.3d 602 (Del. 2021) 17

United States v. Abboud,
438 F.3d 554 (6th Cir. 2006) 19

United States v. Blake,
868 F.3d 960 (11th Cir. 2017) 18

United States v. Cardwell,
680 F.2d 75 (9th Cir. 1982) 8

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 9, 12

United States v. Diaz,
841 F.2d 1 (1st Cir. 1988) 20

United States v. Drebin,
557 F.2d 1316 (9th Cir. 1977) 8

United States v. Galpin,
720 F.3d 436 (2d Cir. 2013) 14

United States v. Hill,
459 F.3d 966 (9th Cir. 2006) 7, 8

United States v. Hillyard,
677 F.2d 1336 (9th Cir. 1982) 8

United States v. Jones,
565 U.S. 400 (2012) 13

United States v. Kow,
58 F.3d 423 (9th Cir. 1995) 8

United States v. Mercery,
591 F. Supp. 3d 1369 (M.D. Ga. 2022) 18

United States v. Morton,
46 F.4th 331 (2022) 16

United States v. Morton,
984 F.3d 421 (5th Cir. 2021) 16

United States v. Otero,
563 F.3d 1127 (10th Cir. 2009) 15

United States v. Payton,
573 F.3d 859 (9th Cir. 2009) 9, 11

United States v. Shipp,
392 F. Supp. 3d 300 (E.D.N.Y. 2019) 11, 17

United States v. Stabile,
633 F.3d 219 (3d Cir. 2011) 21

United States v. Stubbs,
873 F.2d 210 (9th Cir. 1989) 8

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 10

United States v. Wey,
256 F. Supp. 3d 355 (S.D.N.Y. 2017) 16, 17

United States v. Williams,
592 F.3d 511 (4th Cir. 2010) 22

Other Authorities

Apple, *Compare Mac Models* 9

Apple, *macOS User Guide: Set Up Users, Guests, and Groups on Mac* 21

Karen Kent et al., *Guide to Integrating Forensic Techniques Into Incident Response: Recommendations of the National Institute of Standards and Technology*, NIST SP No. 800-86 (Aug. 2006) 23

LexisNexis, *How Many Pages in a Gigabyte* (2007) 9

Microsoft, *Search for eDiscovery Activities in the Audit Log*, Microsoft Docs (Jan. 7, 2022) 24

Press Release, BlackBag, BlackBag Announces Release of BlackLight 2019 R2 (Sept. 5, 2019) 23

Gov. Response to Def.'s Mot. to Suppress Evidence,
United States v. Holcomb, 639 F. Supp. 3d 1142 (W.D. Wash. 2022) 22

Reply to Gov.'s Response to Mot. to Suppress,
United States v. Holcomb, 639 F. Supp. 3d 1142 (W.D. Wash. 2022) 26, 27

Microsoft, *Create a User Account in Windows* 20

Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (Oct. 2020) 23

STATEMENT OF INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles of liberty and equality embodied in the United States Constitution and civil rights laws. The American Civil Liberties Union of Washington Foundation ("ACLU-WA"), a state affiliate of the national ACLU, is a statewide, nonpartisan, nonprofit organization with over 135,000 members and supporters dedicated to the preservation of civil liberties. The ACLU and ACLU-WA have a long history of involvement, both as direct counsel and as *amici curiae*, in cases involving the protection of rights under the Fourth Amendment to the U.S. Constitution, including ensuring those rights remain robust in the face of evolving technology. The ACLU served as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[1] Pursuant to Rule 29(a)(2), counsel for *amici curiae* state that all parties have consented to the filing of this brief. Pursuant to Rule 29(a)(4)(E), counsel for amici curiae certify that no person other than *amici curiae*, their members, or their counsel made a monetary contribution to the presentation or submission of this brief. No current counsel for a party authored this brief in whole or in part.

INTRODUCTION & SUMMARY OF ARGUMENT

In this case, the trial court correctly held that a warrant provision authorizing a search of the Defendant's computer—without limitation—for evidence of "dominion and control" was impermissibly overbroad. Prevailing Fourth Amendment law makes clear that in the vast majority of cases, warrants cannot authorize searches of all contents of a computer when the crime under investigation took place over a limited period of time. Moreover, a search for evidence of "dominion and control"—unnecessary in this case because it was undisputed that the computer belonged to the Defendant—can be limited by date range and file type, thereby ensuring that a search for such evidence with respect to a particular crime does not become a search of everything on a device. Adoption of the government's argument that this provision justified a search of any and every file on the Defendant's computer would set a dangerous and unnecessary precedent. The government's capacious interpretation of "dominion and control" would hand law enforcement an all-purpose code word which it could use to convert any warrant into authorization for a wide-ranging general search of any or all files on a computer or cell phone, a result the Fourth Amendment cannot tolerate.

This conclusion is based on longstanding rules governing and limiting warrants, rules that should be scrupulously followed in the context of digital

searches. Computers now house almost unimaginable amounts of private and sensitive information. That, plus the Fourth Amendment's requirement that searches be both particular and narrow, means that courts must tie what officers can search and seize closely to the probable cause showing for the particular case. None of this is new or surprising to a trained officer—and for that reason, the good faith doctrine should not excuse the government's egregious conduct in this case.

Increasingly, courts have applied Fourth Amendment principles to digital searches by imposing limits on the relevant time-frame and categories of data that law enforcement may search and insisting that police search only data with a close nexus to probable cause. These limits are necessary to avoid fishing expeditions long barred by the Fourth Amendment and to prevent police from exploiting the trove of sensitive digital data stored on computer hard drives, on cell phones, and in online accounts by searching information they are not entitled to search.

This Court should suppress the evidence used against the Defendant because, as would be clear to any reasonable officer, it was obtained in violation of the Fourth Amendment.

FACTS

During the course of their investigation of Holcomb for allegedly raping complainant JJ on the evening of January 27, 2020, officers with the Burlington Police Department obtained a warrant, signed by Judge Riquelme of Skagit County

Superior Court in Washington, to search the Defendant's desktop computer. E.R. 125–26. The warrant was based on Judge Riquelme's finding of probable cause to believe that the computer contained evidence of the alleged rape of JJ. *Id.* Specifically, police believed based on an interview with Holcomb that the computer contained video recordings of the night in question that would confirm or contradict JJ's statements. *Id.* at 133–34. Thus, the warrant authorized police to search for:

> - Evidence of communications to or from JJ and/or between JOHN HOLCOMB, JILL or JJ. This communication includes but is not limited to voicemails/audio recordings, SMS, MMS, emails, chats, social media posts/online forums, contact lists and call logs from June 1, 2019 to current.
>
> - Surveillance video or images depicting JJ or JOHN HOLCOMB and any other surveillance video or images from Jan 26th, 2020 to current.
>
> - Any location data including GPS coordinates from Jan 26th, 2020 to current.
>
> - User search history from the devices to include but not limited to searched words, items, phrases, names, places, or images from Jan 26th, 2020 to current.
>
> - Files, artifacts, or information including but not limited to, documents, photographs, videos, e-mails, social media posts, chats and internet cache that would show dominion and control for the devices.

Id. at 125–26.

The dominion and control clause was almost certainly boilerplate. Holcomb had already told police that the computer belonged to him, and they initially planned

to search it pursuant to his consent, something that would have been improper if they did not already believe that the computer was his. Beyond that, the ownership of the computer was irrelevant to the criminal investigation. The issue at hand was the nature of the sexual encounter between Holcomb and JJ. The computer could have belonged to anyone, and the 2020 video depicting Holcomb and JJ would have been equally probative. These facts make it even more obviously unreasonable for the government to rely on the "dominion and control" clause as justification for the intrusive inspection officers gave to Holcomb's private files, including intimate videos of him and his wife.

Warrant in hand, investigators searched the computer. On February 20, 2020, the forensic examiner determined that the relevant video "raised a legitimate question as to the credibility of the complaining witness' statement." *Id.* at 151. After informing the investigator and prosecutor of that fact, on the morning of February 21, the three men reviewed the relevant video evidence and agreed that there was no evidence that the Defendant had raped JJ. *Id.* at 143, 149. Nevertheless, the prosecutor asked the forensic examiner to continue processing and reviewing data on other hard drives. *Id.* at 143. Later in the day on February 21, the examiner found videos depicting sexual assault of a minor from 2016 and earlier.

Apparently understanding that their search had exceeded the bounds of the Fourth Amendment, local authorities bemoaned having engaged in a constitutional

violation before dismissing their cases and referring the matter to the FBI for possible federal prosecution. *Id.* at 157. The overbroad search would almost certainly have resulted in suppression in Washington, which does not recognize a good faith exception. The move to federal court is an effort to save a search that the government knows is likely to be found, and that the district court did find, unconstitutional.

ARGUMENT

I. Longstanding Fourth Amendment rules prohibit free-ranging searches, including searches of digital information.

A. The Fourth Amendment has long required that warrants clearly limit what officers may seize and police searches must be designed to find relevant information the seizure of which is supported by probable cause.

The Fourth Amendment protects people against unreasonable searches and seizures by requiring that all search warrants be based on probable cause and describe with particularity the places and items to be seized and searched. U.S. Const. amend. IV. These provisions are meant to protect against general warrants, a hated English practice that allowed a general rummaging through the papers and property of anybody suspected of a crime. *See Stanford v. Texas*, 379 U.S. 476, 481 (1965) (general warrants were "the worst instrument of arbitrary power . . . that ever was found in an English law book").

A police officer has probable cause to conduct a search when "the facts available to [him] would 'warrant a [person] of reasonable caution in the belief'

that contraband or evidence of a crime is present." *Florida v. Harris*, 568 U.S. 237, 243 (2013) (alteration in original) (citation omitted). The probable cause requirement protects people in two ways: It ensures there is adequate justification for a search, *see Arizona v. Gant*, 556 U.S. 332, 345 (2009), and it limits the scope of the search based on the warrant, *see United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). This requirement serves the goal of the Fourth Amendment "to place obstacles in the way of a too permeating police surveillance." *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (internal quotation marks and citation omitted).

Search warrants must be particular and narrow in scope. *See, e.g.*, *Stanford*, 379 U.S. at 485 ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another." (citation omitted)); *Berger v. New York*, 388 U.S. 41, 58 (1967) (alteration in original) (citation omitted) (same); *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) ("[T]he warrant . . . was deficient in particularity because it provided no description of the type of evidence sought."); *Kentucky v. King*, 563 U.S. 452, 459 (2011) ("[A] warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity.").

The two requirements of particularity and appropriately narrow breadth are similar, but distinct. "Particularity is the requirement that the warrant must clearly

state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Hill*, 459 F.3d at 973 (citation omitted). The particularity requirement is met "if the warrant imposes a meaningful restriction upon the objects to be seized." *United States v. Cardwell*, 680 F.2d 75 (9th Cir. 1982); *People v. Frank*, 700 P.2d 415, 420 (Cal. 1985). The breadth requirement is met if the warrant constrains invasive "fishing expeditions" by authorizing searches only for evidence of a crime for which there is probable cause. *See Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

A search is unlawfully general where the accompanying warrant "le[aves] to the executing officers," rather than to the magistrate upon issuance, "the task of determining what items f[a]ll within broad categories stated in the warrant" and where there were no clear guidelines distinguishing between property which was subject to search from that which was not. *United States v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982) (citing *United States v. Drebin*, 557 F.2d 1316, 1322–23 (9th Cir. 1977)); *see also United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (warrant listing fourteen categories of business records without limiting descriptions such as names of companies involved in illegal scheme was not sufficiently particular); *United States v. Stubbs*, 873 F.2d 210, 211 (9th Cir. 1989) (lack of probable cause to seize all office documents without reason to believe tax evasion permeated defendant's entire business).

B. Computers and other digital devices contain an immense amount of private, sensitive data.

Digital information generated by today's devices reveals individuals' private matters far beyond what one could learn from physical analogs. *See Riley v. California*, 573 U.S. 373, 394 (2014). Indeed, computers contain far more information of an extremely personal nature than even the most capacious filing cabinet ever could. *See id.* at 394–95; *see also United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam). A digital device the size of a human palm can store practically unlimited quantities of data, *Riley*, 373 U.S. at 394, and computer hard drives can store even more, *see, e.g.*, *United States v. Payton*, 573 F.3d 859, 861–62 (9th Cir. 2009).[2] Moreover, while our garages and desk drawers may fill all the way up with knickknacks, requiring periodic spring cleaning, digital data can infinitely pile up and persist indefinitely.

Because both computers and cell phones "collect[ ] in one place many distinct types of information"—for example, an address, a note, a prescription, a bank statement, or a video—digital data "reveal much more in combination than any isolated record," and much more about "an individual's private interests or concerns." *Riley*, 573 U.S. at 394–95.

[2] Laptops sold in 2023 can store up to eight terabytes of information, the equivalent of more than 5 billion pages of text. *See, e.g.*, Apple, *Compare Mac Models*, https://www.apple.com/mac/compare/; LexisNexis, *How Many Pages in a Gigabyte* (2007), https://perma.cc/HN26-3ZVC.

Thus, law enforcement access to electronically stored data exposes years'—even decades'—worth of personal information. *See Carpenter*, 138 S. Ct. at 2218; *Riley*, 573 U.S. at 394. This combination of volume, depth, and longevity of personal information raises strong privacy risks because in aggregate, digital information reveals much more than the sum of each part. *See Riley*, 573 U.S. at 394.

In some cases, technology has also given law enforcement the ability to obtain previously unobtainable information, *Carpenter*, 138 S. Ct. at 2217–18, such as Internet browsing history, location history, medical records, extensive conversations in the form of e-mail or text, privileged communications, and associational information. Courts have already recognized some of these categories of information as deserving of particularly stringent privacy protections. *See, e.g.*, *id.* (cell-site location information); *Riley*, 573 U.S. at 395–96 (search and browsing history "could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD"); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (medical tests); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (e-mail). As the Supreme Court has explained, the "immense storage capacity" of smartphones and computers allows them to function as "cameras, video players, rolodexes, calendars, tape

recorders, libraries, diaries, albums, televisions, maps, or newspapers," and to store extensive historical information related to each functionality. *Riley*, 573 U.S. at 393.

Indeed, the search of computer devices "would typically expose to the government far more than the most exhaustive search of a house," not least because they "contain[] a broad array of private information *never* found in a home in any form" prior to the digital age. *Id.* at 396–97. As this Court has explained, "searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers." *Payton*, 573 F.3d at 861–62.[3]

C. The overbreadth and particularity provisions of the Fourth Amendment are especially important when officers search electronic information.

The particularity requirement means that a valid warrant to search for a rifle in someone's home does not allow officers to open a medicine cabinet where a rifle could not fit. *Horton v. California*, 496 U.S. 128, 141 (1990). When it comes to searches of digital information, such physical distinctions are no longer a clear

[3] In addition, searches of computers or other digital devices that are connected to the Internet present risks that law enforcement searching through a device could access not just locally stored physical media, but also online accounts. *See, e.g.*, *United States v. Shipp*, 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019) (Police access to social media accounts and online communications services presents a "threat [that] is further elevated . . . because, perhaps more than any other location—including a residence, a computer hard drive, or a car—[they] provide[] a single window through which almost every detail of a person's life is visible.").

guardrail. Computer hard drives and online accounts contain huge amounts of personal information that will inevitably intermingle material that is entirely irrelevant to a criminal investigation with, potentially, evidence of crime. The need to search large quantities of electronic records "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *CDT*, 621 F.3d at 1176.

As a result, in the digital age, courts must take even greater care to ensure that digital searches do not "become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.* at 1177. The Fourth Amendment's originating principles are more important than ever as guides for courts and police tasked with balancing law enforcement's legitimate need to search for evidence of a crime against the countervailing prohibition against general warrants. As technology lowers the barriers to extreme privacy invasions and investigatory overreach, the Fourth Amendment ensures that the longstanding balance between the power and authority of the state and the privacy and liberty of the individual does not, either suddenly or through creep, fall unconstitutionally out of whack. *See, e.g.*, *Berger*, 388 U.S. at 56 ("The need for particularity . . . is especially great in the case of eavesdropping" because such surveillance "involves an intrusion on privacy that is broad in scope.").

In cases involving law enforcement's use or exploitation of emerging

technologies, 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." *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (internal quotation marks and citation omitted). This analysis "is informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (alteration in original) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)); *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001). Courts must ensure that technological innovation does not allow the government to encroach on the degree of privacy the Fourth Amendment was adopted to protect. *See Carpenter*, 138 S. Ct. at 2214 (cell-site location information); *Kyllo*, 533 U.S. at 34–35 (thermal imaging).

II. Traditional Fourth Amendment principles make clear that probable cause to search or seize some data on a digital device does not justify access to the totality of the device's contents.

Given the vast amounts of personal data stored on digital media, and all that can be gleaned from that data, a growing number of courts are making clear that strict limits on digital searches and seizures are crucial to preserve privacy. There is no need for, and the Fourth Amendment does not allow, "all-content" warrants demanding seizure of whatever account content or digital files might exist. Looking for the specific data supported by probable cause, not *any* data, is the only search

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 generic categories of data for which there was no probable cause was "constitutionally intolerable").

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 117 (quoting *Riley*, 573 U.S. at 399). Warrants require probable cause and particularity precisely because searching information not demonstrably likely to be evidence of the crime under investigation is not permitted, even when the object containing that information is lawfully seized.

Like the *Hughes* court, other courts have highlighted the importance of particularity and constraint when conducting digital searches. *See, e.g.*, *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (discussing the need for "heightened

sensitivity to the particularity requirement in the context of digital searches" due to the vast amount of information that digital devices contain); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (ability of a computer to store "a huge array" of information "makes the particularity requirement that much more important"); *see also, e.g.*, *State v. Mansor*, 421 P.3d 323, 326 (Or. 2018) (holding that "warrant[s] must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used," and that warrants must describe, to the greatest degree of specificity possible, the data for which there exists probable cause so as to prevent law enforcement from "rummaging" indiscriminately through the vast amount of sensitive information stored on cell phones); *State v. Wilson*, 884 S.E.2d 298, 300–01 (Ga. 2023) (suppressing evidence obtained from a warrant that authorized a search of all the information on two cell phones for "evidence connected with the crimes.").

Overbroad warrants lack probable cause and are unconstitutional. For example, probable cause to investigate a crime which took place over a one-day period does not permit a search of over eight months of cell phone data. *People v. Thompson*, 178 A.D.3d 457 (N.Y. App. Div. 2020); *see also People v. Musha*, 131 N.Y.S.3d 514, 683 (N.Y. Sup. Ct. 2020) (probable cause to search Internet use history does not amount to probable cause to search a cell phone). Similarly, a warrant that purported to

permit a search of the entirety of a phone's contents for evidence of a crime which allegedly took place over a two-day period was too broad and thus not supported by probable cause. *State v. Missak*, 299 A.3d 821 (N.J. Super. Ct. App. Div. 2023). *See also United States v. Morton*, 984 F.3d 421 (5th Cir. 2021) (government properly obtained a warrant to search a cell phone for text messages, call logs, and contacts, but that warrant did not establish probable cause to believe the evidence would be in the form of photographs, which were therefore suppressed), *rev'd on other grounds*, 46 F.4th 331 (2022) (en banc). 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. *State v. McLawhorn*, 636 S.W.3d 210, 242–44 (Tenn. Crim. App. 2020).

On this basis, there is no probable cause supporting warrants that use the phrase "including but not limited to" or list capacious categories of data, as the "dominion and control" clause does here. For example, in *United States v. Wey*, 256 F. Supp. 3d 355 (S.D.N.Y. 2017), the Southern District of New York rejected a warrant to search multiple types and categories of information—all "financial records, notes, memoranda, records of internal and external communications, correspondence, audio tapes[] and video tapes, [and] photographs," among others, *id.* at 386 (internal quotation marks omitted)—that merely pertained to the suspects. As the court explained, because every document seized from the suspect pertains to

the suspect, the warrants did not impose "meaningful parameters on an otherwise limitless search of a defendant's electronic media," and they failed "to link the evidence sought to the criminal activity supported by probable cause" *Id.* at 387 (citation omitted). Thus, the warrants did "not satisfy the particularity requirement." *Id.*

Likewise, the Delaware Supreme Court recently rejected on particularity grounds a warrant that permitted the search and seizure of "any/all data stored by whatever means." *Taylor v. State*, 260 A.3d 602, 609 (Del. 2021). The court explained that "[t]he 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*. at 616.

Other courts have also followed suit. A search warrant that sought an individual's Facebook account information that went far beyond the types of information likely to provide evidence of the specific crime under investigation was not supported by probable cause. *Shipp*, 392 F. Supp. 3d at 303–07 (search warrant to Facebook demanding all personal information, activity logs, photos and videos from the user as well as those posted by others that tag 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); *see also United States v. Blake*, 868 F.3d 960, 973 (11th Cir. 2017) (questioning validity of broad warrant for Facebook content, but deciding case on good faith grounds). So too with a warrant purporting to authorize search of all information in Instagram account. *United States v. Mercery*, 591 F. Supp. 3d 1369 (M.D. Ga. 2022) (suppressing evidence); *State v. Bock*, 485 P.3d 931, 936 (Or. Ct. 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); *In re U.S. Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1139, 1150 (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").

In sum, it is well-established that probable cause to examine some electronic information does not justify a warrant that essentially would permit a search of all stored data, and this conclusion naturally follows from traditional Fourth Amendment caselaw.

III. Warrants must ensure that overseizures of data are not exploited in ways that give law enforcement a windfall simply because potential evidence is digital in nature.

When seizing hard drives or cell phone, investigators obtain more data that can lawfully be searched under a warrant's authority. If the government is permitted to seize materials beyond the scope of a properly narrow warrant, and then later exploit the overseizure by examining any files or videos it wishes—as happened in this case—the search evades the particularity requirement so essential to ensuring that searches and seizures are constitutional. Given the intermingled nature of electronic evidence, courts must issue warrants that ensure that law enforcement's subsequent searches of that data will be cabined to probable cause. In other words, warrants must be written to ensure that electronic searches do not become data windfalls for law enforcement. Date, file type, and other limitations are crucial in the digital age, and they are easy for courts to impose and police to follow.

A. Courts should limit searches by time frame to ensure they do not expand beyond data relevant to the crime under investigation.

Warrants can easily limit data searches and seizures by time frame. For example, if an offense allegedly took place in June of 2019, police need not view videos from any other month, nor data from much before or after the date when ownership of the hard drives is relevant. *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 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).

B. Courts should limit searches by file type to ensure they do not expand beyond data relevant to the crime under investigation.

Information whose search is justified by probable cause must still be limited to the types of data likely to reveal that information. Thus, if a warrant authorizes a search of digital data to show ownership—or, like in this case, "dominion and control"—there will be other forms of searchable data more than capable of demonstrating ownership, as opposed to more private data that theoretically might disclose the same thing. For example, on a machine running the Windows operating system, the "User Accounts" menu displays users' account name and associated e-mail address, information directly relevant to who has access to the computer, as well as what files they can access.[4] And on an Apple Mac laptop, the System Preferences "Users & Groups" and "Internet Accounts" menu lists similar data.[5] It

[4] *See* Microsoft, *Create a User Account in Windows*, https://support.microsoft.com/en- us/windows/create-a-user-account-in-windows-4fac6fd5-74c0-9737-69b8-6e77e00422dc.

[5] *See* Apple, *macOS User Guide: Set Up Users, Guests, and Groups on Mac*,

is hard to imagine how the additional videos investigators watched in this case could be more probative of "dominion and control" over Holcomb's computer than a list of user accounts and e-mail addresses would have been.

C. Forensic tools make it straightforward for law enforcement to narrow searches by file type, date range, and other limitations that adhere closely to probable cause.

Contrary to some government claims, officers need not perform a file-by-file review of the data on a suspect's computer in every case. Doing so is impossible. Review of every file in suspects' online accounts or on their hard drives will often be counterproductive, for it is impractical for an investigator to manually review the hundreds of thousands of images, files, and messages stored there. It is also unnecessary, giving law enforcement too much discretion. Given that investigators *will* exercise discretion, it is incumbent on courts issuing warrants to guide those decisions.

In some older cases, courts have held that because criminals could hide or mislabel files, expansive searches of digital information were both practically necessary and permissible under the Fourth Amendment. *See, e.g.*, *United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011); *see also United States v. Williams*, 592

---

https://support.apple.com/guide/mac-help/set-up-other-users-on-your-mac-mtusr001/mac.

F.3d 511, 521 (4th Cir. 2010).[6] But these assertions are premised on an outmoded understanding of today's technology. An accurate understanding of modern technology should defeat the government's argument in this case that any data on Holcomb's computer is fair game to prove dominion and control. Gov. Response to Def.'s Mot. to Suppress Evidence at 13, 25–27, *United States v. Holcomb*, 639 F. Supp. 3d 1142 (W.D. Wash. 2022), ECF No. 41.

Modern forensics tools, widely available today for both criminal investigations and e-discovery, can search data for file type, dates, and keywords, all without revealing the contents of non-responsive documents to a human reviewer.

> Fortunately, various tools and techniques can be used to reduce the amount of data that has to be sifted through. Text and pattern searches can be used to identify pertinent data, such as finding documents that mention a particular subject or person, or identifying e-mail log entries for a particular e-mail address. Another helpful technique is to use a tool that can determine the type of contents of each data file, such as text, graphics, music, or a compressed file archive. Knowledge of data file types can be used to identify files that merit further study, as well as to exclude files that are of no interest to the examination. There are also databases containing information about known files, which can also be used to include or exclude files from

[6] In some cases, when a suspect is using sophisticated techniques to hide data, it may make sense to give officers increased leeway in their search to find potentially hidden information. But in such a scenario, there should be a probable cause showing of the actor's "sophisticated" nature— perhaps, for example, the suspect is a skilled computer programmer who knows how to manipulate data. But since the scope of a warrant must be limited by probable cause, if a suspect is not shown to be sophisticated, there will be no reason to believe that relevant evidence will be found in files or places not specifically connected to probable cause.

further consideration.

Karen Kent et al., *Guide to Integrating Forensic Techniques Into Incident Response: Recommendations of the National Institute of Standards and Technology*, NIST SP No. 800-86, § 3.2 (Aug. 2006), https://perma.cc/Y2N7-K65R.

There are many such products on the market and available to law enforcement at the state and local level, as well as to the FBI. Forensic Tool Kit and Cellebrite are just two examples. The Blacklight tool claims to categorize both still images and videos as related to alcohol, child sexual abuse material ("CSAM"), currency, drugs, extremism, gambling, gore, porn, swim/underwear, and weapons.[7] Research by the organization Upturn shows that mobile device forensic tools are widely available even to smaller law enforcement agencies, which either purchase them outright, obtain them through federal grants, or work with larger local law enforcement agencies that conduct extractions of data at the smaller agencies' request.[8]

Forensic tools may also help courts exercise their constitutional responsibility to oversee searches. Many forensic tools have a search history feature, just as eDiscovery tools do.[9] Such query or audit logs facilitate a post-search review to ensure law

[7] Press Release, BlackBag, BlackBag Announces Release of BlackLight 2019 R2 (Sept. 5, 2019), https://www.blackbagtech.com/press-releases/blackbag-announces-release-of-blacklight-2019-r2.

[8] *See* Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (Oct. 2020), https://perma.cc/7DCK-PGMQ.

[9] *See, e.g.*, Microsoft, *Search for eDiscovery Activities in the Audit Log*, Microsoft

enforcement complied with the dictates of the warrant. With such logs, judges could better understand the precise steps that law enforcement took when searching a cell phone. In particular, these logs could equip judges to better assess the reasonableness of the search technique and ascertain if the search was sufficiently narrowly tailored to the warrant. If courts were to insist upon the production of digital audit logs created by the forensic tool upon the return of a search warrant, tool vendors that do not already provide this functionality would rapidly develop this feature.

Without some reason to believe that the computer data was manipulated by someone sophisticated enough to elude forensic tools, courts should not presume that there is good cause for investigators to examine whichever information they like on a device. In *State v. Missak*, the state sought to justify an all-content warrant to search a cell phone on the grounds that any defendant may alter computer files and thereby hide information relevant to the crimes for which probable cause has been established. The New Jersey appellate court found this justification was not constitutionally sufficient because probably cause requires a higher standard than what may potentially occur. There would have to be some information supporting a

---

Docs (Jan. 7, 2022), https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log?view=o365-worldwide (explaining that content search and eDiscovery-related activities are logged in the audit log when creating, starting, and editing Content searches, and performing search actions, such as previewing, exporting, and deleting search results, among other activities).

belief that the data had been manipulated. 299 A.3d 821.

In sum, forensic search tools can make searches limited by date and file type workable, while also being effective for law enforcement. Proper warrants and judicial oversight can ensure that these powerful tools are 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. Certainly, limiting searches by file category or type will not always be possible—but it often is, and in those situations, this Court should require that warrants indicate, and officers observe, that limitation.

IV. Officers should have known that the search that turned up the relevant evidence in this case violated the Fourth Amendment, and the good faith exception should not apply.

That viewing videos from years before the alleged offense is outside the scope of any legitimate warrant is common sense. A need to search for evidence of "dominion and control" over a computer does not and cannot justify police examination of any or all information stored there. *See supra* Part II. Otherwise, mere inclusion of the phrase "dominion and control" would permit an essentially boundless examination of all of a computer's contents, threatening to turn all digital searches into unconstitutional general ones. A reasonably well-trained officer should have known that this provision of the warrant was impermissibly broad, and that the search investigators conducted was well beyond the bounds of probable cause.

And here, there was no need to establish ownership of the machine. The record is replete with police references to the device at issue as the Defendant's computer, and the police seized it and planned to search it based on his consent—something that would have been improper without a reason to believe it was his machine. Reply to Gov.'s Response to Mot. to Suppress at 17–18 & n.12, *Holcomb*, 639 F. Supp. 3d 1142, ECF No. 49. Even if dominion and control were genuinely an issue in the case, a warrant permitting a search of "Files artifacts or information (sic) including but not limited to, documents" and other broad categories is overbroad and not sufficiently particularized. *See id.* at 13–18.

Moreover, as explained above, *see supra* Part III.A., the "dominion and control" authorization should have included a date range relevant to the case, as did the other warrant provisions. For example, it should have limited searches to indicia of dominion and control in January of 2020. It also should have identified specific, narrow categories of data closely tied to ownership and usage. Officers could have been limited to searching system preferences for a list of user accounts, which generally include identifiers such as an e-mail address. They could have looked to see what e-mail or social network accounts were logged in on the machine (without review the contents of those messages), or what logins were stored in a password saver. Any of these categories of data, which show that a defendant logs in to the computer and checks his e-mail there, are more probative of ownership, custody, and

control of the computer than merely appearing in a video recorded by cameras in the home. After all, JJ and Holcomb's wife appeared in videos, but it was not their computer.

Indeed, police in this case may have viewed some of the most private and intimate information imaginable, videos of the Defendant and his wife having sex, going back as far as 2015, as well as conversations between the two in which they discussed their sex life. Reply to Gov.'s Response to Mot. to Suppress at 18, 38, *Holcomb*, 639 F. Supp. 3d 1142. But law enforcement had no legitimate authority to look at that information in order to investigate the Defendant for a rape that allegedly occurred in January of 2020.

As demonstrated above, well-established legal precedent compels the conclusion that the "dominion and control" clause could not authorize a plenary search of the computer. As a result, the good faith exception does not apply. *See, e.g.*, *Wilson*, 884 S.E.2d at 301 (declining to apply GFE when warrant purported to authorize search of "any and all stored electronic information" on two cell phones).

CONCLUSION

For these reasons, the Court should hold that the search in this case was unconstitutional.

DATED this 20th of November, 2023

/s/ *Jennifer Stisa Granick*
Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
E-mail: jgranick@aclu.org

Brett Max Kaufman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
E-mail: bkaufman@aclu.org

Jazmyn Clark
AMERICAN CIVIL LIBERTIES
UNION OF WASHINGTON
FOUNDATION
P.O. Box 2728
Seattle, WA 98111
Tel: (206) 624-2184
E-mail: jclark@aclu-wa.org

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I served the foregoing Brief of *Amici Curiae*, on counsel for all parties, electronically through the ACMS System, on this 20th day of November, 2023.

DATED this 20th of November, 2023 /s/ *Jennifer Stisa Granick*
Jennifer Stisa Granick

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 23-469

I am the attorney or self-represented party.

This brief contains 6,612 **words,** including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - ☐ it is a joint brief submitted by separately represented parties.
  - ☐ a party or parties are filing a single brief in response to multiple briefs.
  - ☐ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated ____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature /s/ Jennifer Stisa Granick **Date** November 20, 2023
*(use "*s/[typed name]*" to sign electronically-filed documents)*