The Honorable Judge Robert S. Lasnik

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. JOHN HOLCOMB., Defendant.	CASE NO. CR21–75–RSL [PROPOSED] BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION AND AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON IN SUPPORT OF DEFENDANT JOHN HOLCOMB'S MOTION TO SUPPRESS

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

TABLE OF CONTENTS

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

TABLE OF AUTHORITIES

CASES

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

OTHER AUTHORITIES

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

I. INTRODUCTION & SUMMARY OF ARGUMENT

Courts should apply longstanding rules governing and limiting warrants scrupulously in the context of digital searches because almost any search of a device's digital data can easily morph into a search of all the data on the device—and the Fourth Amendment prohibits general warrants. 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. Modern courts have recognized this, imposing limits on the relevant categories of data that can be searched, ensuring that time frames apply to the data searched, and insisting on a close nexus between probable cause and the data to be searched. These limits are necessary to avoid police 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.

In this case, police discovery of the video evidence was unconstitutional for two reasons. First, at the time police discovered these videos, officers no longer had probable cause to search Holcomb's computer for evidence of rape—and no warrant authorized a search for evidence of any other crime. Second, the warrant provision authorizing a search for evidence of "dominion and control" was overbroad. Adoption of the government's argument that the provision justified a search of any and every file on Holcomb's computer would set a dangerous precedent. Indeed, the government's capacious interpretation would give law enforcement a code word with which it could turn every warrant into an unconstitutional general one. A search for evidence of "dominion and control"—a need that does not appear to even been at issue in this case because it

AMERICAN CIVIL LIBERTIES UNION OF
WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

was clear and undisputed that the computer belonged to the defendant—can be limited by date range and file type, thereby ensuring that a search for evidence of a particular crime does not become a search of everything on a device.

II. 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. Dkt. #35-1 at 45–46. 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 53–54. Thus, the warrant authorized police to search for:

1. 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.

2. Surveillance video or images depicting JJ or JOHN HOLCOMB and any other surveillance video or images from Jan 26th, 2020 to current.

3. Any location data including GPS coordinates from Jan 26th to current.

4. 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.

5. 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 45–46.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

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 71. 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 63, 69. Nevertheless, the prosecutor asked the forensic examiner to continue processing and reviewing data on other hard drives. *Id.* at 63. Later in the day on February 21, the examiner found videos depicting sexual assault of a minor from 2016 and earlier. *Id.* at 69; Dkt. #41 at 6.

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. Dkt. #35-1 at 77.

III. ARGUMENT

A. Courts must scrupulously apply longstanding Fourth Amendment rules regarding limits on warrants to searches of digital information to ensure that digital searches do not morph into unconstitutional general searches.

1. 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

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

data, *id*., and computer hard drives can store even more, *see, e.g.*, *United States v. Payton*, 573 F.3d 859, 861–62 (9th Cir. 2009).[1] Moreover, while our garages and desk drawers may fill all the way up with knickknacks, requiring periodic spring cleaning, digital data can 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," *Riley*, 573 U.S. at 394, and they reveal much more about "an individual's private interests or concerns." *Id.* at 395. Thus, law enforcement access to electronically stored data exposes years'—even decades'—worth of personal information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018); *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 email 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.*, *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

[1] Laptops sold in 2021 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.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

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) (email). 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 the Ninth Circuit 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.[2]

2. The Fourth Amendment requires that warrants to search digital data be scrupulously particular and narrow.

a. *Warrants must clearly limit what officers may seize and police searches must be designed to find relevant information whose seizure 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. US Const. amend. IV. These provisions are meant to

[2] 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 more than locally stored physical media but online accounts, too. *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 present 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.").

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

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). 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*, 138 S. Ct. at 2214 (citation and quotation marks omitted).

Search warrants must also 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) ("The Fourth Amendment's requirement that a warrant 'particularly describ(e) the place to be searched, and the persons or things to be seized,' repudiated these general warrants and 'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another.'" (alteration in original)); *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

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

unless probable cause is properly established and the scope of the authorized search is set out with particularity.").

The two requirements of "particularity and 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 (citations 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*, 38 Cal. 3d 711, 724 (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).

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

Police must search only within the parameters of the warrant, and only when there is probable cause. If police violate the terms of the warrant, the search is unconstitutional, absent some exception to the warrant requirement.

b. *Adhering to constitutional requirements about overbreadth and particularity is especially important when officers search electronic information.*

The particularity requirement is more easily understood when applied during searches of physical spaces. For example, 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. *See*, *e.g.*, *Horton v. California*, 496 U.S. 128, 141 (1990). Circumventing that limitation was not only unlawful, but often obvious.

When it comes to searches of digital information, physical distinctions are no longer a clear guardrail. Computer hard drives and online services contain huge amounts of personal information that will inevitably intermingle material that is entirely irrelevant to a criminal investigation and, potentially, evidence of criminal behavior. 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." *CDT*, 621 F.3d at 1177. 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." *Id*. at 1176.

The Fourth Amendment's originating principles are more important than ever as guides for courts tasked with balancing law enforcement's legitimate need to search for evidence of a crime on one hand, and the countervailing prohibition against general warrants and their evils. As technology lowers the barriers to extreme privacy invasions and investigatory overreach, the

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

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 constitutionally 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) (quotation marks 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).

B. In case after case, courts are imposing limits on warrants in recognition that probable cause to search or seize some data on a digital device cannot 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. 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

AMERICAN CIVIL LIBERTIES UNION OF
WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

court rejected the state's extreme argument

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

Id. at 541–42 (quoting *Riley*, 573 U.S. at 399). 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. Like the *Hughes* court, other courts have begun to impose similar limitations on 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 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).

A district court case from Michigan helpfully illustrates how courts are now managing these issues. In *United States v. Stetkiw*, the government alleged, and the court was concerned, that "individuals might hide information in a way that forces a protocol-bound investigator to

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

overlook it." No. 18-20579, 2019 WL 2866516, at *5 (E.D. Mich. July 3, 2019). Nevertheless, the court held that "an *ex ante* 'minimization' requirement can address concerns about potential Fourth Amendment violations of protocol-less searches, with a goal of decreasing the amount of non-responsive [electronically stored information] encountered in a search." *Id.* (citing Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 Emory L.J. 49, 55 (2018)). The court concluded that *ex ante* procedures would have several advantages:

> First, it can minimize the need for *ex post* review of those procedures, which is often contentious as parties debate motions to suppress evidence in criminal cases. Second, it allows a magistrate judge to closely work with the Government to ensure its preferred procedures do not violate the Fourth Amendment. Third, it can promote the development of case law that can distinguish permissible and impermissible procedures to better protect Fourth Amendment rights. Finally, it could prevent situations where certain file locations are authorized for search by warrant, but the practical implications of that authorization create a general warrant without the magistrate judge's knowledge.

Id. While the *Stetkiw* court did not maintain that *ex ante* protocols must be required in every case, it did suggest that in order to escape the need for such protocols, the government "should demonstrate that the level of probable cause to search [electronically stored information] is high enough to justify a search without minimization." *Id.*

1. Courts can and should impose limitations on the categories of data to be searched on a digital device.

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. Rather than issue "all-content" warrants, courts should authorize seizure only of relevant categories of data that are supported by probable cause. Looking for the right data, not for *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 categories of data for which there was no probable cause was "constitutionally intolerable").

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

Thus, for example, probable cause to search for photographs does not amount to probable cause to search for web history. *People v. Musha*, 131 N.Y.S.3d 514, 683 (N.Y. Sup. Ct. 2020); *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), *vacated and reh'g en banc granted*, 996 F.3d 754 (5th Cir. May 18, 2021). 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*, No. M2018-02152-CCA-R3-CD, 2020 WL 6142866, at *24–*26 (Tenn. Crim. App. Oct. 20, 2020).

Along these lines, one federal court rejected 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 and were unconnected to probable cause. *See United States v. Shipp*, 392 F. Supp. 3d 300, 303–07 (E.D.N.Y. 2019) (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).

Similarly, courts are rejecting warrants that use the phrase "including but not limited to" or list capacious categories of data, as the fifth provision of the warrant here does. 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,

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

audio tapes[] and video tapes, [and] photographs," among others, *id.* at 386 (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. Thus, the warrants did "not satisfy the particularity requirement." *Id.*

Likewise, the Delaware Supreme Court recently rejected a warrant, on particularity grounds, 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 followed suit. *See, e.g.*, *State v. Bock*, 485 P.3d 931, 936 (Or. App. 2021) (warrant authorizing the search of a cell phone for circumstantial evidence about the owner and any evidence related to suspected criminal offenses, including unlawful firearm possession, was not sufficiently specific under state constitution's Fourth Amendment corollary); *In re United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 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").

Finally, 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

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

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 could disclose the same thing. For example, on a machine running the Windows operating system, the "User Accounts" menu displays users' account name and associated email address, information directly relevant to who has access to the computer, as well as what files they can access.[3] And on an Apple Mac laptop, the System Preferences "Users & Groups" and "Internet Accounts" menu lists similar data.[4]

2. 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." (citations omitted)); *United States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure records before the first instance of wrongdoing mentioned in the affidavit); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no warrant issued where government did not include a date limitation); *In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application without date restriction denied as overbroad).

[3] *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.

[4] *See* Apple, *macOS User Guide: Set up users, guests, and groups on Mac*, https://support.apple.com/guide/mac-help/set-up-other-users-on-your-mac-mtusr001/mac.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

3. 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. Some prosecutors have argued and some courts have held that because criminals can hide or mislabel files, expansive searches of digital information are 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 F.3d 511, 521 (4th Cir. 2010).[5] Indeed, the government here argues that any data on Holcomb's computer is fair game to prove dominion and control. Dkt. #41 at 13, 25–27. But these assertions are premised on an outmoded understanding of today's technology. Indeed, 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.

Instead, 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

[5] 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.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

> 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 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.

Forensic tools may have a search history feature, just as eDiscovery tools do.[6] Such query or audit logs facilitate a post-search review to ensure law 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.

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 ToolKit 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,

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

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

Swim/Underwear, and Weapons.[7] Research by the firm 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]

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.

C. Courts have additional options to 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, but then later exploit the overseizure by examining any files or videos it wishes—as happened in this case—it undermines the particularity requirement so essential to ensuring that searches and seizures are constitutional.

---

[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.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

Because of this, courts can and should issue warrants that ensure that law enforcement's subsequent searches of that data will be cabined to probable cause. In other words, courts should ensure that electronic searches do not become data windfalls for law enforcement.

1. Courts should strictly limit any applications of the plain view doctrine to digital searches.

In its opposition brief, the government suggests that the search of the video evidence in this case would be justified by the plain view doctrine. Dkt. #41 at 13. But the plain view doctrine, especially if applied as broadly as the government suggests could be done here, would seriously threaten to turn every digital search into an unconstitutional general one. Indeed, that threat is present here, because the government asserts that even if investigators have ulterior motives in conducting their searches, they can search every video (and other files) and use whatever they find. *Id.* at 14.

To avoid unconstitutional general searches, the Fourth Amendment must ensure that investigators do not take advantage of the unique properties of digital storage and reap a windfall by opening non-responsive files and discovering evidence of some other crime, as took place here. The plain view doctrine developed in cases involving physical-world searches, where evidence is tangible and discrete. But electronic searches are a poor fit for the plain view exception because the justifications underlying the exception are, by and large, absent in this context. *See e.g., Bock*, 483 P.3d 931 (holding plain view exception cannot be reconciled with the Oregon Constitution's Fourth Amendment analogue in the context of electronic searches). First, officer safety is not implicated in a controlled environment like an off-site forensics laboratory. *See generally* David H. Angeli & Christina M. Schuck, *The Plain View Doctrine and Computer Searches: Balancing Law Enforcement's Investigatory Needs with Privacy Rights in*

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

the Digital Age, 34 Champion 18, 23 (Aug. 2010). Unlike a physical object, such as a knife or gun, *see, e.g.*, *United States v. Bishop*, 338 F.3d 623, 628–29 (6th Cir. 2003), the digital data stored on a computer hard drive can physically endanger no one. *See Riley*, 573 U.S. at 386–87. Second, evidence preservation is not at risk in a typical computer search, which normally begins with seizure of the computer and its data and extraction of the data stored on the hard drive. Third, where the computer hard drive is preserved pending execution of the warrant, the police have ample time to obtain additional warrants (say, for permission to expand the search or for evidence of an unrelated crime) without risking evidence destruction. *See, e.g.*, Christina M. Schuck, Note, *A Search for the Caselaw to Support the Computer Search "Guidance" in* United States v. Comprehensive Drug Testing, 16 Lewis & Clark L. Rev. 741, 760–61 (2012).

2. Courts should impose use restrictions on seized data.

To ensure that broad digital searches adhere to Fourth Amendment principles, courts should exclude evidence police stumble upon, and impose a general use restriction on any non-responsive data obtained in an electronic search and seizure. *Mansor*, 421 P.3d at 343–45 (holding that the State may not use information obtained in a computer search in a prosecution if the warrant did not authorize the search for that information, unless some other warrant exception applies); *see also* Orin Kerr, *Executing Warrants for Digital Evidence*, 48 Tex. Tech. L. Rev. 1, 8 (2015); Rebecca Lipman, *Protecting Privacy with Fourth Amendment Use Restrictions*, 25 Geo. Mason L. Rev. 412 (2018). The doctrinal reasoning behind this view is that, although the seizure of non-responsive files is reasonable when needed to effectuate the search for responsive files, retention of the files is an ongoing seizure. While initially justified, the subsequent use of seized non-responsive files transforms the nature of the seizure and renders it constitutionally unreasonable. *Id*. at 25–29. Even when a search is reasonable, the government

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

should be required to delete materials that were not the object of the search once they have been segregated. *See CDT*, 621 F.3d at 1177 (discussing the need to segregate nonresponsive information).

Courts now are implementing versions of these solutions. For example, in Vermont, magistrates may design and supervise "targeted searches" by "restricting law enforcement's search to those items that met certain parameters based on dates, types of files, or the author of a document." *See In re Search Warrant*, 71 A.3d 1158, 1184 (Vt. 2012); *see also 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").

As one federal judge put it, "[i]t is almost always possible to characterize the Fourth Amendment as an inconvenience to law enforcement officials as they carry out their vital duties," but "[t]hat inconvenience . . . is one of the fundamental protections that separates the United States of America from totalitarian regimes." *Doe v. Prosecutor*, 566 F. Supp. 2d 862, 887 (S.D. Ind. 2008). *See also Johnson v. United States*, 333 U.S. 10, 15 (1948); *United States v. Morgan*, 743 F.2d 1158, 1163–64 (6th Cir. 1984); *United States v. Diggs*, 544 F.2d 116, 130 (3d Cir. 1976).

D. In this case, the search that turned up the relevant evidence violated the Fourth Amendment.

The government's search in this case was unconstitutional under the Fourth Amendment for two reasons. First, no probable cause existed to continue searching Holcomb's computer. And second, the warrant at issue did not authorize and could not have authorized the search that uncovered the video evidence at issue in this case.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

First, at the point that the prosecution team realized the video of Holcomb's sexual encounter with JJ was exculpatory and that he had committed no crime, they should have stopped their search. At that point, there was no longer probable cause, and probable cause is essential in defining a permissible scope of searches of electronic data. *See supra* Part III.A.2.a.

Probable cause must exist not only at the time law enforcement obtains a warrant, but at the time the warrant is executed as well. Where a search warrant is issued on probable cause, changed circumstances or new information can weaken or even entirely negate a prior determination of probable cause. *See United States v. Bizier*, 111 F.3d 214, 219 (1st Cir. 1997) (intervening information can weaken probable cause); *United States v. Jacobs*, 986 F.2d 1231, 1235 (8th Cir. 1993) (finding new information can negate prior determination of probable cause). Execution of a warrant violates the Fourth Amendment if, between the time of issuance and the time of execution, probable cause becomes stale or dissipates. Police "may not disregard facts tending to dissipate probable cause." *Nicholson v. City of Los Angeles*, 935 F.3d 685 (9th Cir. 2019). When new circumstances call into question an original finding of probable cause, the officer must bring the new information to the issuing magistrate's attention. *United States v. Bowling*, 900 F.2d 926, 933 (6th Cir. 1990); *State v. Maddox*, 98 P.3d 1199, 1203–04 (Wash. 2004). An officer has a duty to report the new information to the magistrate if "the information is material to the magistrate's determination of probable cause." *United States v. Marin-Buitrago*, 734 F.2d 889, 894 (2d Cir. 1984). For example, there may initially be probable cause justifying an arrest, but additional information obtained at the scene may indicate that there is less than a fair probability that the defendant has committed or is committing a crime. In such cases, execution of the arrest or continuation of the arrest is illegal. *United States v. Lopez*, 482 F.3d 1067, 1073 (9th Cir. 2007).

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

Here, the prosecutor's failure to call off the search resulted in an invasive search without probable cause, or at least without the magistrate's independent finding that the Fourth Amendment requires. U.S. Const. amend. IV. The forensic examiner, at least, appears to have viewed videos depicting Holcomb having sex with his wife while searching despite knowing that the probable cause that had formed the basis of the warrant was stale.

Second, the government argues that the investigators' examination of the videos at issue in this case was lawful because the warrant authorized searches for evidence of "dominion and control." Dkt. #41 at 12–16. However, 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 III.C.1–2. 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.

As an initial matter, there was really no question in this case that the computer belonged to the Defendant. The record is replete with police references to the device at issue as the Defendant's computer, and the police seized it based on his consent—something that would have been improper without a reason to believe it was his machine. Dkt. #49 at 17–18 & n.12. 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.[9]

Moreover, as explained above, *see supra* Part III.C.1–2, the "dominion and control"

[9] Oddly, the government asserts that "the warrant issued did not include the 'including, but not limited to' language that Holcomb finds so problematic." Dkt. #41 at 24. It does. Dkt. #35-1 at 46.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

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 June of 2019. 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 email address. They could have looked to see what email 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 email 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 Jill appeared in videos, but it was not their computer.

Date, file type, and other limitations are crucial in the digital age, and they are easy for courts to impose and police to follow. Other parts of the warrant properly used date limitations that should have ensured that old emails or photographs contained on a seized device were not unnecessarily searched. Similar limitations on warrant clause five should have prevented law enforcement from encroaching upon private information whose review was *not* connected to probable cause of rape and discovering the relevant evidence in this case.

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. Dkt. #49 at 18, 38. But law enforcement had no legitimate authority to look at that information in order to investigate the defendant for a rape that occurred in January of 2020.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
P.O. BOX 2728
SEATTLE, WA 98111
(206) 624-2184

IV. CONCLUSION

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

DATED this 15th day of April, 2022.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION

By: s/*Nancy Talner*
Nancy L. Talner, WSBA 11196
P.O. Box 2728
Seattle, WA 98111
Tel: (206) 624-2184
E-mail: talner@aclu-wa.org

Counsel for Amici Curiae

AMERICAN CIVIL LIBERTIES UNION FOUNDATION

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

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

**Admitted Pro Hac Vice*