12-240-cr

IN THE

United States Court of Appeals

FOR THE SECOND CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

—against—

STAVROS M. GANIAS,

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NEW HAVEN DISTRICT OF CONNECTICUT

BRIEF FOR *AMICI CURIAE* CENTER FOR DEMOCRACY & TECHNOLOGY, AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF CONNECTICUT, BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW, ELECTRONIC FRONTIER FOUNDATION, AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE IN SUPPORT OF DEFENDANT-APPELLANT

TANYA L. FORSHEIT
BAKER & HOSTETLER LLP
11601 Wilshire Boulevard, Suite 1400
Los Angeles, California 90025
(310) 442-8831
tforsheit@bakerlaw.com

WILLIAM W. HELLMUTH
BAKER & HOSTETLER LLP
1050 Connecticut Avenue, NW, Suite 1100
Washington, DC 20036
(202) 861-1703
whellmuth@bakerlaw.com

Attorneys for Amicus Curiae
Center for Democracy & Technology

(*For Continuation of Appearances See Inside Cover*)

July 29, 2015

ALEX ABDO
NATHAN FREED WESSLER
JASON D. WILLIAMSON
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, New York 10004
(212) 549-2500
aabdo@aclu.org

DAN BARRETT
AMERICAN CIVIL LIBERTIES UNION OF CONNECTICUT
330 Main Street, 1st Floor
Hartford, Connecticut 06106
(860) 471-8471
dbarrett@acluct.org
* Not admitted in Connecticut

FAIZA PATEL
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
161 Sixth Avenue, 12th Floor
New York, New York 10013
(646) 292-8335
faiza.patel@nyu.edu

HANNI FAKHOURY
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
hanni@eff.org

LAURA M. MOY
OPEN TECHNOLOGY INSTITUTE | NEW AMERICA
1899 L Street, NW, Suite 400
Washington, DC 20036
(202) 986-2700
moy@newamerica.org

Attorneys for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rules 26.1 and 29(c) of the Federal Rules of Appellate Procedure, *amici* state as follows:

The Center for Democracy and Technology has no parent company and has issued no stock. Thus, no publicly held corporation owns 10% or more of Center for Democracy and Technology stock.

The American Civil Liberties Union has no parent company and has issued no stock. Thus, no publicly held corporation owns 10% or more of American Civil Liberties Union stock.

The American Civil Liberties Union of Connecticut is an affiliate of the American Civil Liberties Union. No publicly held company owns 10% or more of its stock.

The Brennan Center for Justice is an institute affiliated with the New York University School of Law. No publicly held company owns 10% or more of its stock.

The Electronic Frontier Foundation has no parent company and has issued no stock. Thus, no publicly held corporation owns 10% or more of Electronic Frontier Foundation stock.

New America's Open Technology Institute is a program of New America. No publicly held company owns 10% or more of its stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

Amici Curiae are non-profit public interest organizations seeking to protect speech, privacy, and innovation—and access to speech and new technologies—on the Internet.

The Center for Democracy & Technology (CDT) is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated and emerging technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty in the digital world. It pursues that interest in the policy arena, and in the courts by filing briefs *amicus curiae* in cases that include *Riley v. California*, 134 S. Ct. 2473 (2014) (searches of cellular telephones incident to arrest); *United States v. Jones*, 132 S. Ct. 945 (2012) (warrantless GPS tracking involving physical trespass); and *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (extraterritorial warrants).

[1] This amicus brief is filed with consent of the parties to this case. No party's counsel authored any portion of this brief, nor did any party or party's counsel contribute money intended to fund this brief's preparation or submission. No persons other than the *amici*, their members, or their counsel contributed money that was intended to fund this brief's preparation or submission.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's civil rights laws. The American Civil Liberties Union of Connecticut ("ACLU-CT") is the affiliate of the ACLU in the State of Connecticut. Together and independently, the ACLU and the ACLU-CT have appeared numerous times before the federal courts in cases involving the Fourth Amendment, including, in particular, cases involving the right to privacy in the digital age. For example, the ACLU is or was counsel in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) (FISA Amendments Act surveillance), *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (bulk collection of call records), and *United States v. Katzin*, 769 F.3d 163 (3d Cir. 2014) (warrantless GPS tracking), and it served as *amicus curiae* in *United States v. Jones*, 132 S. Ct. 945 (2012) (warrantless GPS tracking), *Riley v. California*, 134 S. Ct. 2473 (2014) (cellphone searches incident to arrest), and *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (warrantless acquisition of cellphone location information).

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice, including access to the courts and constitutional limits on the government's exercise of power. The Center's Liberty and National Security (LNS) Program

uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic counterterrorism policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on privacy and First and Fourth Amendment freedoms. As part of this effort, the Center has filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008); and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008). The Brennan Center's views as amicus curiae in this case do not and will not purport to represent the position of NYU School of Law.

The Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization based in San Francisco, California, working to protect innovation, free speech, and privacy in a digital world. With more than 22,000 active donors nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. As part of its mission, EFF has served as amicus curiae in landmark cases addressing Fourth Amendment issues raised by emerging technologies. *See*,

e.g., *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc); *In re Application of the U.S. For Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

New America's Open Technology Institute ("OTI") is a program of New America dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open communications networks. OTI, through its unique blend of policy expertise, technical capacity, and field-level engagement, seeks to promote a stronger and more open Internet to support stronger and more open communities. Digital Fourth Amendment policy and law is a particular area of interest for OTI, and the Institute testifies before Congress regularly on issues of digital privacy and surveillance, as well as before the Judicial Conference Advisory Committee on Criminal Rules on the topic of Federal Rule of Criminal Procedure 41. New America is a non-profit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences.

SUMMARY OF ARGUMENT

The Founders crafted the Fourth Amendment as a shield against unjustified or overreaching invasions into the privacy of individuals. In this case, the government threatens to upend that protection in the digital realm by ignoring key constitutional constraints on its authority to search or seize digital data. Specifically, the government argues that the Fourth Amendment permits it to seize vast quantities of data that has nothing to do with its investigation, to retain that data indefinitely, and to later search it in an entirely unrelated investigation. Taken to its logical conclusion, the government could amass a gigantic repository of every digital file it comes across that shares hard-drive space with files to which it is actually entitled, and then years later revisit people's most private personal records in aid of some new suspicion or case. This argument ignores the Fourth Amendment's requirements of particularity and reasonableness, and the Court should reject it. The Court should, instead, clarify two principles of law that would ensure that the Fourth Amendment's protections remain as robust in the digital world as they are in the physical world.

First, the Court should hold that the copying of digital data is a search and seizure under the Fourth Amendment. The circuit courts that have considered this question, including the panel in this case, have unanimously held as much, and for good reason. The copying of digital data places in government hands

extraordinarily sensitive information, in which individuals have a reasonable expectation of privacy. It also deprives the owner of critical possessory interests in the data: the exclusive use of it and the ability to delete it. Moreover, the copying of digital data by law enforcement serves precisely the same governmental purpose as any traditional search and seizure—namely, to secure evidence. A contrary rule—that the copying of digital data does not trigger the Fourth Amendment—would have devastating consequences for privacy by giving the government carte blanche to copy and store individuals' data without any constitutional constraint.

Second, the Court should hold that, when the government seizes entire hard-drives of data to facilitate particularized searches, the Fourth Amendment forbids the government from retaining any non-responsive data for longer than reasonably necessary to effectuate its search. In this case, after copying several entire hard-drives of data, the government retained the data collected for an unreasonably long period of time, even after it had separated the data responsive to the original warrant from the non-responsive data. The government had no justifiable reason for retaining the nonresponsive data, and its retention was therefore unconstitutional under the Fourth Amendment.

The panel in this case noted that not only do "Fourth Amendment protections apply to modern computer files" but, "[i]f anything, even greater protection is warranted." *United States v. Ganias*, 755 F.3d 125, 135 (2d Cir.

2014) (citations omitted). The Court should affirm these principles to ensure that, despite rapid changes in technology, the protections of the Fourth Amendment remain steadfast and strong.

ARGUMENT

I. The Copying of Digital Data Constitutes a Search and Seizure under the Fourth Amendment.

The panel opinion correctly held that the government's copying of the defendant's personal records "was a meaningful interference with [his] possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment." *Ganias*, 755 F.3d at 137 (citations omitted). The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. Here, the government's copying of the defendant's hard-drives triggered the Fourth Amendment for two independent reasons: (1) it was a search because it placed in government hands information in which the defendant had a reasonable expectation of privacy; and (2) it was a seizure because it deprived the defendant of the exclusive use of his records. This Court should affirm the panel's conclusion—which is consistent

with the conclusion of every other circuit court to have addressed the question—that the copying of data triggers Fourth Amendment protections.

First, the copying of data constitutes a search within the meaning of the Fourth Amendment. In *Katz v. United States*, Justice Harlan stated in his concurring opinion that where "a person has a constitutionally protected reasonable expectation of privacy, . . . electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment." 389 U.S. 347, 360 (1967) (Harlan, J., concurring). The courts have built upon Justice Harlan's logic, and now recognize that "the ultimate touchstone of the Fourth Amendment is reasonableness." *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (citations omitted). The Supreme Court has recognized that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361). Thus, a search within the meaning of the Fourth Amendment has occurred when law enforcement conducts an electronic intrusion into an environment where an individual has an actual expectation of privacy that society is prepared to recognize as reasonable.

The first question in this case, then, is whether the government invaded a reasonable expectation of privacy when it copied the entirety of Mr. Ganias's hard-drives. It unquestionably did. Individuals reasonably expect that the government

will not take for its own purposes personal data stored privately on their computers. *See, e.g.*, *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("[i]ndividuals generally possess a reasonable expectation of privacy in their home computers" (collecting cases)). Further, in *Leventhal v. Knapek*, this Court concluded that an employee had a reasonable expectation of privacy in his personal files that were stored on his work computer. 266 F.3d 64, 72-74 (2d Cir. 2001). Here, Mr. Ganias likewise held a reasonable expectation of privacy in his files, particularly his personal files, which the government intruded upon when making the forensic copies of his computers.

There is no question that, had the government retained Mr. Ganias's actual hard-drives, it would have invaded a reasonable expectation of privacy. There should also be no question that, when the government accomplishes the same ends by creating a mirror copy of the hard-drive, the government has likewise invaded a reasonable expectation of privacy.

Second, and independently, the copying of data constitutes a seizure within the meaning of the Fourth Amendment. "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (citations omitted). The government's copying of data interferes with at least two possessory interests: (1) the right to exclude others; and (2) the right to dispose of property.

As Justice Stevens wrote in *United States v. Karo*, "[t]he owner of property, of course, has a right to exclude from it all the world, including the government, and a concomitant right to use it exclusively for his own purposes." 468 U.S. 705, 729 (1984) (Stevens, J., concurring in part, dissenting in part); *see also eBay v. MercExchange, L.L.C.*, 547 U.S. 388 (2006) (explaining that, in the patent infringement context, the essence of an ownership right is the right to exclude others from accessing a thing). And as this Court has observed more recently, "[t]he rights and benefits of property ownership . . . include not only the right to actual possession of a thing, but also the right to exclude others from possessing it, the right to use it and receive income from its use, the right to transmit it to another, and the right to sell, alienate, waste, or even destroy it." *Almeida v. Holder*, 588 F.3d 778, 788 (2d Cir. 2009) (citing Hon. James L. Oakes, "*Property Rights" in Constitutional Analysis Today*, 56 Wash. L. Rev. 583, 589 (1981)).

The copying of digital data divests owners of these central possessory interests by preventing them from exercising absolute control over their data. It denies them the ability to exclude others from using their data, and it prevents them from disposing of their data as they see fit. Therefore, the act of copying this data meaningfully interferes with an individual's possessory interests in the data, constituting a seizure under the Fourth Amendment.

The panel in this case reached this same conclusion. "Th[e] combination of circumstances [in this case] enabled the government to possess indefinitely personal records of Ganias that were beyond the scope of the warrant while it looked for other evidence to give it probable cause to search the files. This was a meaningful interference with Ganias's possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment." *Ganias*, 755 F.3d at 137 (citing *United States v. Place*, 462 U.S. 696, 708 (1983) (detaining a traveler's luggage while awaiting the arrival of a drug-sniffing dog constituted a seizure); *Soldal v. Cook Cnty*., 506 U.S. 56, 62-64, 68 (1992) (explaining that a seizure occurs when one's property rights are violated, even if the property is never searched and the owner's privacy was never violated); *Loretto v. Teleprompter Manhattan CATV Corp*., 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights.")). Other circuits have reached similar conclusions. *See United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam) (referring to the copying of electronic data as a seizure throughout the opinion); *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002) (describing information retrieved by the government with assistance of Yahoo! technicians from two email accounts as a "seizure").

For these reasons, this Court should reaffirm the panel holding that the copying of digital data triggers ordinary Fourth Amendment protections. As explained more fully below, any other rule would have catastrophic consequences for privacy.

II. The Retention of Digitally Copied Data Beyond the Scope of a Warrant is Unconstitutional under the Fourth Amendment.

Because the government's copying of Mr. Ganias's data constitutes a search or seizure under the Fourth Amendment, it must comply with the Fourth Amendment's warrant and reasonableness requirements. It did not in this instance.

First, the government retained data beyond the scope of its original warrant long after it had effectuated that warrant. As a general matter, the particularity requirement of the Fourth Amendment mandates that the government's searches and seizures be particular, or limited to the information, individuals, and places for which it can justify a search or seizure. *Marron v. United States*, 275 U.S. 192, 196 (1927) ("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. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

In the digital context, courts have often permitted the government to *over*-seize data—that is, to seize data beyond the scope of its warrant—in order to facilitate its more targeted searches. Courts have permitted over-seizure as a

prophylactic to accommodate the government's claim that on-site review of digital data would be infeasible in certain circumstances.[2] *Comprehensive Drug Testing*, 621 F.3d at 1177 (recognizing "the reality that over-seizing is an inherent part of the electronic search process and [it will] proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records"); *see also Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) (recognizing that over-seizure is sometimes appropriate, but cautioning against unwarranted intrusions into an individual's privacy). Even if the constitutional requirement of particularity permits that prophylactic, it does not permit the government to *profit* from it. The government may not convert that accommodation into a free license to retain data for which it would not independently have had probable cause to collect and search in the first place.

The Supreme Court has "long held . . . that the purpose of the particularity requirement is not limited to the prevention of general searches. . . . A particular warrant also assures the individual whose property is searched or seized of the

[2] Such a broad seizure may, itself, be unconstitutional, if there are narrower alternatives available. Indeed, given the severity of the invasion of the mirroring of a hard-drive, courts should insist upon clear evidence of the need for such a drastic measure. If they nonetheless approve of mirroring, courts should spell out the authority clearly in the warrant being issued, along with specific guidance and restrictions on the government's ability to search the media at issue and a clear statement on the government's obligation to promptly purge any data not within the scope of the warrant.

lawful authority of the executing officer, his need to search, and the limits of his power to search." *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (citations omitted). Thus, in cases of electronic over-seizures, the government must limit its review and retention of computer files to those which it truly needs to search. *See Andresen*, 427 U.S. at 482 n.11; *Comprehensive Drug Testing*, 621 F.3d at 1177 (calling for "greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures"). The government may not, in other words, read the particularity requirement out of the Constitution. To give that requirement meaning in the digital context, this Court should make clear that, when the government over-seizes digital data, it may not retain data unresponsive to its warrant beyond the full execution of its warrant or the time reasonably necessary to execute the warrant.

Second, even if the particularity requirement did not apply, the government's retention of data unresponsive to its warrant long after it had effectuated that warrant would be unreasonable. "[T]he ultimate touchstone of the Fourth Amendment" is "reasonableness." *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Reasonableness is determined by examining the "totality of the circumstances" to "assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to

which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 171 (2008).

Here, the totality of the circumstances clearly demonstrates the unreasonableness of permitting the government to retain data long after it had effecuated its warrant. The government's retention of Mr. Ganias's records constituted a severe intrusion into the privacy of his papers, and the government had no legitimate interest in retaining data unresponsive to its warrant.

As a preliminary matter, it is uncontested that in 2004 the government was able to identify those materials from the seized computers that were responsive to the original warrant. Thus, the government created two distinct data sets: one set consisting of materials that were responsive to the 2003 warrant and a second set consisting of materials that were not responsive, but which contained Mr. Ganias's personal files, among other documents. *Ganias*, 755 F.3d at 137-38. Mr. Ganias holds strong possessory and privacy interests in these files, particularly his personal files.

The government made a series of arguments as to why its retention and use of this nonresponsive data set was reasonable; however, as the panel noted, none of these arguments were persuasive. *See id*. at 138-40. Of the government's arguments, only the claim that returning or destroying the non-responsive files

would compromise the remainder of the copied data appeared to demonstrate any actual interest in the non-responsive data set itself. *See id*. at 139. However, that rationale makes little sense: there ought to be any number of ways of preserving the evidentiary value of the responsive data seized without holding onto vast quantities of other data. As the panel stated, "[w]e are not convinced that there is no other way to preserve the evidentiary chain of custody. But even if we assumed it were necessary to maintain a complete copy of the hard-drive solely to authenticate evidence responsive to the original warrant, that does not provide a basis for using the mirror image for any other purpose." *Id.*

Moreover, the government compounded the intrusion into Mr. Ganias's personal data by retaining the data it seized for an additional one and a half years after it had fully executed its initial warrant, and by then searching the data yet again in an *unrelated* investigation. *See United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998) ("[E]ven a seizure based on probable cause is unconstitutional if police act with unreasonable delay in securing a warrant.").

Failure to recognize the copying of digital data by law enforcement as the equivalent of other forms of search and seizure would resurrect the "chief evil that prompted the framing and adoption of the Fourth Amendment": permitting general warrants. *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013). As this Court explained in *Galpin*, the Fourth Amendment was adopted in response to "the

'indiscriminate searches and seizures' conducted by the British 'under the authority of 'general warrants.'" *Id*. (citing *Payton v. New York*, 445 U.S. 573, 583 (1980); *Arizona v. Gant*, 556 U.S. 332, 345 (2009) ("[T]he central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person's private effects.")). Therefore, a ruling that digital copying is not protected under the Fourth Amendment risks permitting unfettered gathering and warehousing of data by the government. It would enable the government to amass and maintain an enormous catalog of electronic communications and data that can later be reviewed if and when probable cause (or some other perceived justification) arises.

This is not an idle concern, particularly given the government's posture in this case. Here, the government claimed that, after creating the mirror images of Mr. Ganias's computers, those mirror images became "the government's property," which it was under no obligation to return or purge. *See Ganias*, 755 F.3d at 129. The government took this untenable position despite the fact that the mirror imaged copies are full of non-responsive (and almost certainly confidential and private) information, well outside the scope of the initial warrant under which the information was gathered. Going forward, as law enforcement copies more and more data in its investigations (in the cloud and beyond), this legal position will carry with it an ever greater threat to privacy in the digital age.

Moreover, the government's over-seizure of digital information is not unique to this case. It has frequently taken the position that the over-seizure of digital data is necessary to allow it to identify files and documents responsive to its warrants. *See, e.g.*, *Galpin*, 720 F.3d at 447 ("As the Ninth Circuit has explained, because there is currently no way to ascertain the content of a file without opening it and because files containing evidence of a crime may be intermingled with millions of innocuous files, '[b]y necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.'" (citing *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176)). It is quickly becoming the norm for the government to seize extraordinary amounts of digital data in the pursuit of narrow amounts of information. The government is poised, in other words, to create even more large stockpiles of information to be searched later, if and when needed, as it did in this case.

In *Andresen v. Maryland*, the Supreme Court recognized that there are "grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable." 427 U.S. at 482 n.11. These dangers are particularly present in executing warrants addressing digital information, where a search will implicate not only great volumes of

"papers," but an unprecedented diversity of private information as well. *See Riley*, 134 S. Ct. at 2489 ("[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. [And] a cell phone's capacity allows even just one type of information to convey far more than previously possible."). Critically, the Supreme Court in *Andresen* observed that the "State was correct in returning [papers that were not within the scope of the warrants or were otherwise improperly seized] voluntarily [to the owner]," and that the "trial judge was correct in suppressing others." 427 U.S. at 482 n.11. The Court cautioned that, when faced with searches and seizures of this scope, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Id*.

Without a rule recognizing the copying of data as a search and seizure under the Fourth Amendment, the government might be tempted to gather information from individuals at its leisure, without a warrant, until such a time that the information might be needed. The end result of that would be a return to the very sort of activity that the Fourth Amendment was drafted to combat: indiscriminate collection of personal information by the government.

The government has failed to demonstrate a legitimate interest in retaining the non-responsive data set, let alone an interest sufficient to justify an intrusion into a constitutionally protected right. Once the government separated the responsive documents under the 2003 warrant from the non-responsive documents, the retention of the non-responsive documents became unreasonable and, as such, a violation of Mr. Ganias's Fourth Amendment rights.

III. The Court Should Decide the Constitutional Questions Presented Whether or Not It Determines that Suppression is Warranted.

Regardless of whether suppression is ultimately warranted, this Court should address the novel and important Fourth Amendment questions raised in the instant case. An analysis of a good-faith reliance argument—which is an *exception* to the exclusionary rule—often requires courts to determine whether a Fourth Amendment violation occurred in the first place. *Illinois v. Gates*, 462 U.S. 213, 264-65 (1983) (White, J., concurring) ("Indeed, it may be difficult to determine whether the officers acted reasonably until the Fourth Amendment issue is resolved."). But even if the Court *could* decide the case solely by addressing the good-faith exception to the exclusionary rule, it should not do so in light of the pressing need for judicial guidance on the underlying Fourth Amendment questions.

Federal, state, and local law enforcement agencies increasingly rely on searches of electronic devices, frequently carried out by making mirror image

copies of voluminous quantities of data. Yet, law enforcement agents and members of the public in this Circuit—as in others—lack guidance regarding the Fourth Amendment limits on such searches and the protections due to copied data once obtained. There is an acute need for guidance from this Court now, and that need will increase over time. Addressing the good-faith exception without also deciding the underlying Fourth Amendment question will deprive the public and the government of such guidance and result in "Fourth Amendment law . . . becoming ossified." *Davis v. United States*, 131 S. Ct. 2419, 2433 (2011).

As the Sixth Circuit has explained:

> If every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the Government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations. In other words, if the exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries.

United States v. Warshak, 631 F.3d 266, 282 n.13 (6th Cir. 2010). Thus, "[w]hen a Fourth Amendment case presents a novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates, there is sufficient reason for the Court to decide the violation issue *before* turning to the good-faith question." *Gates*, 462 U.S. at 264 (White, J., concurring).

Indeed, the practice of reviewing substantive Fourth Amendment questions before turning to suppression or good faith is routine, including by this Court. *See*,

e.g., *United States v. Clark*, 638 F.3d 89, 91 (2d Cir. 2011); *United States v. Otero*, 563 F.3d 1127, 1131–33 (10th Cir. 2009); *United States v. Davis*, 785 F.3d 498, 513, 518 n.20 (11th Cir. 2015) (en banc).

In granting *en banc* rehearing, this Court has already recognized the importance and novelty of the constitutional questions presented. *See* Fed. R. App. P. 35 (stating that *en banc* rehearing must not be ordered except where "the proceeding involves a question of exceptional importance"); *Watson v. Geren*, 587 F.3d 156, 160 (2d Cir. 2009) ("*En banc* review should be limited generally to only those cases that raise issues of important systemic consequences for the development of the law and the administration of justice."). Because courts in this Circuit (and in others) are without guidance on Fourth Amendment questions surrounding the copying and retention of data, and because this area involves novel and important technological questions, the Court should decide the constitutionality of the search and seizure at issue. Doing so is necessary to ensure that technological advances do not "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34.

CONCLUSION

For the foregoing reasons, the Court should affirm that the copying of digital data constitutes a search and seizure under the Fourth Amendment and that the

government's retention and later search of Mr. Ganias's data that fell outside the scope of the 2003 subpoena was unconstitutional.

Dated: July 29, 2015

Respectfully submitted,
/s/ William W. Hellmuth

Tanya L. Forsheit
BAKER & HOSTETLER, LLP
11601 Wilshire Boulevard, Suite 1400
Los Angeles, California 90025
(310) 442-8831
tforsheit@bakerlaw.com

William W. Hellmuth
BAKER & HOSTETLER, LLP
1050 Connecticut Avenue, NW, Suite 1100
Washington, DC 20036
(202) 841-1059
whellmuth@bakerlaw.com

Counsel for Amicus Curiae The Center for Democracy and Technology

Alex Abdo
Nathan Freed Wessler
Jason D. Williamson
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
aabdo@aclu.org

Dan Barrett
AMERICAN CIVIL LIBERTIES UNION OF CONNECTICUT
330 Main Street, 1st Floor
Hartford, CT 06106
(860) 471-8471
dbarrett@acluct.org
* Not admitted in Connecticut

Faiza Patel
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
161 Sixth Avenue, 12th Floor
New York, New York 10013
(646) 292-8335
faiza.patel@nyu.edu

Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
hanni@eff.org

Laura M. Moy
OPEN TECHNOLOGY INSTITUTE | NEW AMERICA
1899 L Street, NW, Suite 400
Washington, DC 20036
(202) 986-2700
moy@newamerica.org

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 5,445 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman font.

Dated: July 29, 2015 /s/ William W. Hellmuth

William W. Hellmuth

BAKER & HOSTETLER, LLP
1050 Connecticut Avenue, NW, Suite 1100
Washington, DC 20036
202) 841-1059
whellmuth@bakerlaw.com

Counsel for Amicus Curiae The Center for Democracy and Technology

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Second Circuit by using the appellate CM/ECF system on July 29, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 29, 2015 /s/ William W. Hellmuth

William W. Hellmuth

BAKER & HOSTETLER, LLP
1050 Connecticut Avenue, NW, Suite 1100
Washington, DC 20036
202) 841-1059
whellmuth@bakerlaw.com

Counsel for Amicus Curiae The Center for Democracy and Technology