12-240-cr

In the United States Court of Appeals for the Second Circuit

UNITED STATES OF AMERICA,

Appellee,

v.

STAVROS M. GANIAS,

Defendant-Appellant.

On Appeal from the United States District Court
for the District of Connecticut

BRIEF OF *AMICUS CURIAE*
RESTORE THE FOURTH, INC.
in Support of Defendant-Appellant Stavros M. Ganias

Mahesha P. Subbaraman
SUBBARAMAN PLLC
222 S. 9th Street, Suite 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

Counsel for Amicus Curiae
Restore the Fourth, Inc.

Corporate Disclosure Statement

In accordance with the requirements of Rule 26.1 of the Federal Rules of Appellate Procedure, the undersigned counsel certifies that Restore the Fourth, Inc. is a nonprofit corporation incorporated under Massachusetts law and is further registered under Section 501(c)(4) of the Internal Revenue Code. Restore the Fourth, Inc. has no parent corporation or shareholders who are subject to disclosure.

Dated: July 29, 2015

s/ *Mahesha P. Subbaraman*

Mahesha P. Subbaraman
SUBBARAMAN PLLC
222 S. 9th Street, Suite 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

Counsel for Amicus Curiae
Restore the Fourth, Inc.

Table of Contents

Page

Table of Authorities

Page

Cases

Table of Authorities (cont'd)

Page

Cases (cont'd)

Table of Authorities (cont'd)

Page

Cases (cont'd)

Table of Authorities (cont'd)

Page

Cases (cont'd)

Other Authorities

Table of Authorities (cont'd)

Page

Other Authorities (cont'd)

Amicus Identity, Interest, and Authority to File

1. Identity of Restore the Fourth, Inc.[1]

Restore the Fourth, Inc. ("Amicus") is a national, non-partisan civil rights organization dedicated to ending all forms of unconstitutional government surveillance. Amicus believes that all Americans are entitled to security in their persons, homes, papers, and effects. Amicus therefore works to increase public awareness of laws and police practices that undermine the Fourth Amendment. In this regard, Amicus has led peaceful rallies in support of the Fourth Amendment in dozens of major U.S. cities. Amicus also assists a diverse network of 26 local chapters in their efforts to bolster grassroots political support for the Fourth Amendment.

2. Interest of Restore the Fourth

Amicus cares about this case because it stands to affect the privacy of Americans in their digital papers for generations to come. The "sum of an individual's private life can be reconstructed" through one's digital papers,

[1] In compliance with Federal Rule of Appellate Procedure 29(c)(5) and Second Circuit Local Rule 29.1(b), Amicus certifies that no party nor counsel for any party in this case: (1) wrote this brief in part or in whole; or (2) contributed money meant to fund the preparation or submission of this brief. Only Amicus, including its members and counsel, has contributed money to fund the preparation and submission of this brief.

whether stored on a modern cellphone or a computer hard drive. *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). Hence, when the government searches or seizes such digital papers, close judicial oversight is required, especially since "unconstitutional practices get their first footing … by silent approaches and slight deviations from legal modes of procedure." *Boyd v. United States*, 116 U.S. 616, 635 (1886).

For this reason, Amicus believes the panel majority in this case correctly concluded that: (1) the Fourth Amendment does not permit the government to indefinitely detain a person's digital papers when these papers are not responsive to a lawful warrant; and (2) enforcement of this principle in this case required evidentiary suppression. *United States v. Ganias*, 755 F.2d 125, 133–41 (2d Cir. 2014). Indeed, if the government may keep copies of one's digital papers indefinitely without a warrant, then no American can ever be truly secure in their digital papers.

3. Authority of Restore the Fourth to File

Amicus files this brief under: (1) this Court's June 29, 2015 Order granting *en banc* review in *Ganias* and "invit[ing] amicus curiae briefs from interested parties"; and (2) Federal Rule of Appellate Procedure 29(a), with all parties in this case having consented to the filing of this brief.

Summary of the Argument

The Fourth Amendment guarantees the right of every American to be secure from unreasonable governmental searches and seizures of their private papers, be they physical or digital in form. The Fourth Amendment further guarantees that any warrant authorizing a government search or seizure of private papers will be carefully limited in scope.

Digital papers, however, lack the "physical dimensions" that would otherwise naturally impose Fourth Amendment limits on "where an officer may pry." *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). The police may thus copy and indefinitely detain every paper on a person's hard drive at negligible cost—except to the Fourth Amendment.

Based on this reality, a divided panel of this Court held that the indefinite detention of a defendant's non-responsive digital papers violated the Fourth Amendment and merited evidentiary suppression. In rehearing this case *en banc*, this Court should reaffirm that holding. By doing so, this Court will ensure that the Fourth Amendment continues to protect "the right most valued by civilized men": the "right to be let alone." *Olmstead v. United States*, 277 U.S. 438, 478(1928) (Brandeis, J., dissenting).

Argument

1. When the government detains digital papers that are not responsive to a lawful warrant, it commits a serious violation of the Fourth Amendment.

A. There exists a strong privacy interest in maintaining exclusive possession of one's digital papers.

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Papers are mentioned for good reason. One of the greatest threats to liberty in the Framers' time was the "general warrant," which gave British authorities free rein to seize "books and papers that might be used to convict their owner." *Boyd v. United States*, 116 U.S. 616, 626 (1886). And against this threat stood *Entick v. Carrington*—a landmark British case that invalidated general warrants. *See id.* The Supreme Court has since characterized *Entick* as "a wellspring of the rights now protected by the Fourth Amendment." *Stanford v. Texas*, 379 U.S. 476, 484 (1965).

The facts of *Entick* are simple. John Entick was the author of a publication deemed seditious by the state. *See id.* at 483. Messengers of the King were consequently authorized to seize Entick's papers—a command they executed in November 1762 by "ransack[ing] Entick's home for four

hours and cart[ing] away quantities of his books and papers." *Id.* at 483–84. Entick then sued these messengers for trespass. *Boyd*, 116 U.S. at 626. In 1765, Lord Camden announced a judgment in Entick's case that made clear what was at stake: the power of the state to seize all of a person's papers, such that "[h]is house is rifled" and "his most valuable secrets are taken out of his possession." *Stanford*, 379 U.S. at 484 (quoting *Entick*).

Lord Camden held that such a power was illegal and void. *Boyd*, 116 U.S. at 629. He observed that "[p]apers are the owner's goods and chattels; **they are his dearest property**; and are so far from enduring a seizure, that they will hardly bear an inspection." *Boyd,* 116 U.S. at 628 (quoting *Entick*) (emphasis added). Lord Camden thus recognized that what the state "carrie[s] away" when it seizes a person's "private papers" is not so much the documents themselves but "the secret nature of those goods." *Id.* This, in Lord Camden's view, called for a greater award of damages to Entick than would normally be the case for a trespass onto land. *Id.*

Lord Camden's reasoning confirms the basic reality that private papers (i.e., diaries, journals, notes, letters, etc.) are the literal embodiment of a person's thoughts. That is what makes them a person's "dearest property." Lord Camden's reasoning also confirms that exclusive

possession of one's papers is vital to maintaining their value as property, because otherwise the "secret nature of those goods" is lost.

Two common sense observations support this conclusion. First, exclusive possession is what spurs people to create private papers in the first place. A person who knows that every paper he creates will be read by strangers is less likely to create such papers at all.[2] Second, exclusive possession is what affords people full use and enjoyment of their papers, in terms of being able to choose who sees these papers (e.g., friends versus total strangers) and whether these papers are seen at all (e.g., tossing a rough draft). *See, e.g.*, *Nixon v. Admin. of Gen. Servs.*, 433 U.S. 425, 457 (1977) ("Presidents who have established Presidential libraries have usually withheld matters concerned with family or personal finances, or have deposited such materials with restrictions on their screening.").

As a result, individuals have a strong privacy interest in maintaining exclusive possession of their private papers. *See United States v. Cotterman*,

---

[2] *See* Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* 4 (Digital Fourth Amendment Research & Educ., Working Paper, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564; *see also* PEN, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR (2013), http://www.pen.org/sites/default/files/Chilling%Effects_PEN%20American.pdf.

709 F.3d 952, 957 (9th Cir.2013) (en banc) ("The papers we create and maintain … reflect our most private thoughts and activities."). This interest has only grown stronger in the digital age, which has massively expanded the volume of private papers that Americans may create, store, and share. In this regard, the Supreme Court has observed that it is "misleading shorthand" to describe modern cellphones as mere phones when these devices are also "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley*, 134 S. Ct. at 2489. The modern cellphone can also store "millions of pages of text, thousands of pictures, or hundreds of videos," thus giving it the power to reveal "the sum of an individual's private life." *Id.*

It is likewise "misleading shorthand" to describe the contents of hard drives as mere data, files, or information. Such descriptions obscure what a hard drive really contains: a person's private digital papers, be they diaries in the form of Word documents, ledgers in the form of QuickBooks files, and so forth. To lose exclusive possession over these digital papers, in turn, jeopardizes one's sense of personal integrity and security— as anyone who has ever lost a smartphone or a laptop will attest. In particular, such a loss means not knowing, and not being able to control, who is reading one's

papers or how they are being used. *See Winfield v. Trottier*, 710 F.3d 49, 55 (2d Cir. 2013) ("Reading a person's personal mail is a far greater intrusion than a search for contraband because it can invade a person's thoughts."). For this reason, the Fourth Amendment does not permit the government to deprive a person of exclusive possession of their digital papers beyond the amount of time necessary to execute a lawful warrant.

B. The Fourth Amendment's particularity requirement accordingly forbids the government from detaining digital papers outside of a warrant's lawful scope.

While the Fourth Amendment protects a person's papers "wherever they may be," *Ex parte Jackson*, 96 U.S. 727, 733 (1877), digital papers lack the "physical dimensions" that otherwise limit "where an officer may pry." *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). Digital papers thus carry a greater risk of being seized in the same way that John Entick's papers were raided two centuries ago. *See id.* The question then becomes whether any limits attend the seizure of digital papers when "evidence of a crime may be intermingled with millions of innocuous" digital papers, thus prompting officers to seize every digital paper they can find. *Id.*

The answer lies in the Fourth Amendment's requirement that "no warrants shall issue" but upon an "oath or affirmation … particularly

describing. . . [the] things to be seized." The Framers established this requirement to make "general searches … impossible … [by] prevent[ing] the seizure of one thing under a warrant describing another." *Marron v. United States*, 275 U.S. 192, 196 (1927). This requirement thus forces officers to identify the specific papers in a volume of papers they may seize and then return the rest. *See Weeks v. United States*, 232 U.S. 383, 398 (1914) ("That papers wrongfully seized should be turned over to the accused has been frequently recognized in the early as well as later decisions of the courts."). Otherwise, the "process of segregating [papers] that [are] seizable … [becomes] a vehicle for the government to gain access to [papers] which it has no probable cause to collect." *United States v. Comprehensive Drug Testing, Inc. ("CDT")*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc).

Accordingly, when the government holds on to digital papers after determining they are not responsive to a lawful warrant, it does not merely "retain" these papers. "Retention" implies that such conduct is innocent or innocuous. It is neither. If an innocent bystander to a robbery is kept in a holding cell even after the police have determined that she did not commit the robbery, she is not being "retained" by the police; rather, she is being unlawfully "detained." Likewise, a digital paper is detained so long as it is

in police custody, regardless of whether the paper is a copy or an original. *Cf. United States v. Van Leeuwen*, 397 U.S. 249, 252 (1970) ("[D]etention of mail could at some point become an unreasonable seizure of 'papers' or 'effects' within the meaning of the Fourth Amendment.").

With this in mind, it becomes clear that government-made copies of a person's digital papers are not "government property." *Ganias*, 755 F.3d at 138. As noted above, the Fourth Amendment affords the government a limited license to "detain" a person's digital papers—including by making copies of them—until it has sorted out which papers are responsive to a lawful warrant. But once this task is done, the government's license to keep copies of the non-responsive papers expires. These copies must then be returned or destroyed. As for the copies of the responsive digital papers, those copies are either contraband (e.g., illicit images) or evidence, the latter of which the government is permitted to possess but still does not own. *See United States v. Bein*, 214 F.3d 408, 411 (3d Cir. 2000) ("It is well settled that the Government may seize evidence for use in investigation and trial, but that it must return the property once the criminal proceedings have concluded, unless it is contraband or subject to forfeiture.").

Consequently, the government violates the Fourth Amendment when it continues to detain a person's digital papers after the legal justification for this detention has expired. The Supreme Court's decision this past term in *Rodriguez v. United States* cements this point. 135 S. Ct. 1609 (2015). At issue was "whether police routinely may extend an otherwise-completed traffic stop, absent reasonable suspicion, in order to conduct a dog sniff." *Id.* at 1614. The Court's ruling was unequivocal: "[A] police stop exceeding the time needed to handle the matter for which the stop was made violates the Constitution's shield against unreasonable seizures." *Id.* at 1612. The Court thus made it abundantly clear that a police officer's detention of a motorist for even a few minutes after a fully-completed traffic stop is not permissible under the Fourth Amendment. *See id.* at 1615–16.

The same logic extends to the detention of digital papers. Authority for this detention "ends when [the] tasks tied to [the detention] … are—or reasonably should have been—completed." *Id.* at 1614. At that point, the government must end the detention and return all non-responsive digital papers to their owner. Anything less reduces the Fourth Amendment's particularity requirement "to a form of words," allowing the government to execute every warrant for certain digital papers as a *de facto* general

warrant to detain all of a person's digital papers indefinitely. *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920).

C. When the government detains digital papers outside a warrant's scope, it converts a lawful seizure into a general seizure that risks a host of privacy violations.

Nearly 90 years ago, this Court confronted a Fourth Amendment case in which the government claimed that a defendant's lawful arrest at his home authorized the police to seize all incriminatory papers present within the home. *See United States v. Kirschenblatt*, 16 F.2d 202, 202 (2d Cir. 1926). Writing for the Court, Judge Learned Hand rejected this claim, finding that it was "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him, once you have gained lawful entry." *Id.* at 203.

The same is true when the government claims that a lawful warrant to find and seize **certain** digital papers (i.e., search a man's pockets) allows the government to detain **all** of a person's digital papers indefinitely (i.e., ransack his house). By continuing to detain any digital papers that fall outside the scope of a lawful warrant, the government turns a valid limited seizure into an invalid general one. *Cf. Terry v. Ohio*, 392 U.S. 1, 18–19 (1968) ("[A] search which is reasonable at its inception may violate the

Fourth Amendment by virtue of its intolerable intensity and scope."). This conversion, in turn, poses an enormous risk of privacy violations. *See Galpin,* 720 F.3d at 447 ("The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous.").

Risk of Government Misuse: While detaining non-responsive digital papers, the government might peek at these papers to search for evidence of other wrongdoing. *Cf. CDT,* 621 F.3d at 1180–81 (Bea, J., concurring in part and dissenting in part) (noting how an officer, just by "scrolling right," reviewed steroid test results for hundreds of baseball players despite being authorized to review the results of only ten specific players). Or the government might try to leverage its detention of these papers to coerce defendants. *See, e.g., Carpenter v. Koskinen*, No. 3:13-cv-563, slip op. at *11, 2015 WL 3510300 (D. Conn. June 4, 2015) ("The Government cannot hold the plaintiffs' documents in an attempt to gain leverage over Carpenter in its pending criminal cases against him…."). Either way, the ongoing detention of non-responsive digital papers invites government misuse. And police officers, "while acting under the excitement that attends the capture of persons accused of crime," may find this invitation hard to resist. *United States v. Lefkowitz*, 285 U.S. 452, 464 (1932).

Risk of Jeopardizing Intimate and Privileged Relationships: In considering the Fourth Amendment implications of wiretapping 87 years ago, Justice Brandeis observed that: "Whenever a telephone line is tapped, **the privacy of the persons at both ends of the line is invaded**." *Olmstead*, 277 U.S. at 475 (Brandeis, J., dissenting) (emphasis added). The same is true of the government's detention of non-responsive digital papers today. These papers often reveal not only the owner's private thoughts, but also those of his spouse (e.g., through romantic emails); his children (e.g., through shared photos); his attorney (e.g., through appointment notations in a virtual calendar); his doctor (e.g., through entries in a fitness diary); and many more. Even if the government promises not to read these papers, the "privacy of the persons at both ends" is still far less than what it would be if the government lacked any copy of these papers.

Risk of Theft by Outsiders: Neither police stations, nor the headquarters of the Internal Revenue Service, nor the offices of Army investigators, are hermetically-sealed vaults. Only last month, suspected Russian hackers stole over 100,000 taxpayer returns from IRS servers.[3] The

[3] *See* Chris Frates, *IRS Believes Massive Data Theft Originated in Russia*, CNN (June 4, 2015), http://cnn.it/1RowD46.

privacy and safety of these taxpayers has thus been irrevocably injured, even if they still possess the originals of their tax returns.

This indicates a disturbing reality when it comes to the detention of non-responsive digital papers: such detention needlessly exposes these papers to the risk of being stolen, regardless of the way these papers are stored.[4] Indeed, the magazine of the International Association of Chiefs of Police reports that: "[S]ensitive information … ha[s] been stolen from … police agencies' digital files .... Today many chiefs believe the threat of a cyber attack is quite serious; however, just as many admit that current policies, practices, and technology are not sufficient to minimize their agencies' risk."[5] Given this state of affairs, it is fanciful to believe that the government can indefinitely detain digital papers in total safety.

---

[4] *See, e.g.*, Naomi Martin, *NOPD Practices Put Evidence at 'High Risk of Theft or Misplacement,' IG Finds*, NEW ORLEANS TIMES-PICAYUNE (Dec. 10, 2014), http://s.nola.com/2xT9giX (reporting unexplained disappearance of a laptop from a New Orleans Police Department evidence locker); *see also, e.g.*, Gregory Pratt, *Midlothian Cops Pay Ransom to Retrieve Data from Hacker*, CHICAGO TRIB. (Feb. 20, 2015), http://fw.to/wI0HQkV; Bree Sison, *Swansea Police Pay Ransom After Computer System Was Hacked*, CBS NEWS—BOSTON (Nov. 18, 2013), http://cbsloc.al/1OsbcwM.

[5] Terry Suit (Chief of Police, Hampton, Va.), *Facing the New World of Digital Evidence & Cybersecurity*, THE POLICE CHIEF, Feb. 2014, at 50, 50–51, *available at* http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=3270&issue_id=22014.

Finally, it must be recognized that the privacy risks detailed above do not disappear from view under the Fourth Amendment merely because the government promises to adopt or follow certain rules to lower these risks. "[T]he Founders did not fight a revolution to gain the right to government agency protocols." *Riley*, 134 S. Ct. at 2491. And even when the government imposes rules on itself to avert privacy violations, recent history teaches that privacy violations still occur with alarming frequency.

For example, in August 2013, the *Washington Post* revealed that the "National Security Agency has broken privacy rules … thousands of times each year since Congress granted the agency broad new powers in 2008."[6] A month later, the *Minneapolis Star Tribune* reported on the "[w]idespread misuse" of Minnesota's driver's license database,[7] including the case of a former police officer who received over "$1 million in settlements after 140 or more police employees looked up her [license] photograph following gossip about how her looks had changed due to weight loss."[8]

---

6 Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), http://wpo.st/ACrR0.

7 Eric Roper, *Driver's License Snooping Gets Costly for Taxpayers*, STAR TRIB. (Sept. 12, 2013), http://strib.mn/18D1MKD.

8 Editorial, *Judge Makes Right Call in Minnesota Data Snooping Cases*, STAR TRIB. (Sept. 26, 2013), http://strib.mn/1cXrRWR.

These incidents show that where privacy can be protected by relying on something simpler than officer discretion, it should be. When it comes to the privacy of non-responsive digital papers, such an alternative exists: the government should return these papers (or destroy its copies of them), making it impossible for the privacy violations noted above to occur. *Cf. Riley*, 134 S. Ct. at 2495 (establishing "get a warrant" rule to protect the privacy of cellphones instead of relying on officer discretion).

2. The government does not act reasonably or in good faith when it detains non-responsive digital papers as a matter of general practice.

A. Routine disregard of settled Fourth Amendment law is objectively unreasonable and thus does not satisfy the "good faith exception."

When the government unconstitutionally detains a person's non-responsive digital papers and then tries to use these papers as evidence, suppression may be appropriate "to deter" future Fourth Amendment violations of this kind. *United States v. Raymonda*, 780 F.3d 105, 117 (2d Cir. 2015). The question of when to apply suppression hinges on two factors: (1) whether the violation was caused by the offending officer's own conduct or by his reliance on an external authority; and (2) whether the violation was an isolated act of negligence or part of a general practice.

The "officer's own conduct" factor rests on the Supreme Court's basic observations that "the exclusionary rule is designed to deter police misconduct, rather than to punish the errors of judges and magistrates" and "[p]enalizing the officer for [a] magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *United States v. Leon*, 468 U.S. 897, 916, 921 (1984). The Court thus concluded in *Leon* that suppression was unnecessary where a Fourth Amendment violation was the result of a police officer's good-faith reliance on a warrant erroneously issued by a magistrate. *See id.* at 926.

The Supreme Court has since extended the "officer's own conduct" factor to reject suppression where a Fourth Amendment violation is the proximate result of clerical errors by court employees or police staff in another jurisdiction. *See Herring v. United States*, 129 S. Ct. 695, 704 (2009); *Arizona v. Evans*, 514 U.S. 1, 15–16 (1995). In making these extensions, the Court has also articulated the second main factor that governs suppression: the presence of "systemic errors" versus isolated acts. *Herring*, 129 S. Ct. at 704. Hence, in *Evans*, the Court rejected suppression where the clerical error was of a type that only occurred once every three to four years and was "immediately corrected" when discovered. 514 U.S. at 15–16.

By contrast, in *United States v. Edwards,* the Fourth Circuit held that suppression was "especially appropriate" to address a systemic pattern of highly invasive arrestee strip searches. 666 F.3d 877, 885–87 (4th Cir. 2011). The record showed in particular that "police officers [were] conduct[ing] searches inside the underwear of about 50 percent of arrestees, in the same general manner as the strip search performed on [the defendant]." *Id.* at 886. The Fourth Circuit thus concluded that deterring such police conduct fell "plainly within the purposes of the exclusionary rule." *Id.*

What this ultimately means is that "[t]he reasonableness of a seizure depends … on what **the police in fact do**." *Rodriguez*, 135 S. Ct. at 1616 (emphasis added). And when the facts show that the police have detained a person's non-responsive digital papers indefinitely based on a general practice—rather than isolated negligence or reliance on some external authority—this Fourth Amendment violation requires suppression.

B. Fourth Amendment law governing "papers" binds all seizures of papers, physical or digital.

One additional circumstance in which the Supreme Court has rejected evidentiary suppression is "when the police conduct a search in objectively reasonable reliance on binding appellate precedent." *Davis v.*

United States, 131 S. Ct. 2419, 2434 (2011). This conclusion fits with the "officer's own conduct" factor described above. If an officer's conduct is being guided by binding law—rather than a self-adopted or self-serving police practice—then it is unfair to blame the officer for failing to anticipate that such binding law might later be overturned. *See id.*

The logical corollary of this rule is that where the police execute a search or seizure in disregard or defiance of settled Fourth Amendment law, suppression is merited. This means that in jurisdictions lacking explicit appellate precedent dealing with the detention of non-responsive **digital papers**, the government must still comply with binding Fourth Amendment precedents that cover **papers in general**. For example, under this Circuit's binding precedent, "when items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items." *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988). *Matias* faced facts relating to the seizure of certain physical papers, but there is no reason why *Matias* would not apply **as a matter of law** to digital papers—a reality confirmed by the Supreme Court's seminal Fourth Amendment decisions in *Katz v. United States* and *United States v. Jones*.

Indeed, as the Court observed in *Katz,* the Fourth Amendment's protection of a "reasonable expectation of privacy" governs "not only the seizure of tangible items" but also intangibles like "the recording of oral statements." 389 U.S. 347, 353 (1967). And in *Jones*, the Court held that new technologies like GPS tracking devices do not displace the Court's pre-*Katz* Fourth Amendment jurisprudence protecting "houses, persons, papers, and effects" from trespassory searches and seizures. 132 S. Ct. 945, 949 (2012). On this score, the unlawful detention or copying of a person's papers constitutes a "trespass to chattels."[9] *See Harper & Row, Publishers, Inc. v. Nation Enters.*, 723 F.2d 195, 201 n.5 (2d Cir. 1983).

Katz and *Jones* thus demonstrate that digital papers fit readily within the ambit of general Fourth Amendment law. As such, there is abundant Fourth Amendment law to guide the government in how it handles copies or originals of these papers. For example, consider this Court's decision in *United States v. Riley,* in which this Court held that "a warrant authorizing seizure of records of criminal activity permits officers **to examine** many

[9] Copying is a trespass to chattels because it impairs the "condition, quality, [and] value" of the owner's originals, as these originals no longer afford the owner exclusive possession of his papers. *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (quoting Restatement (Second) of Torts § 218).

papers in a suspect's possession **to determine** if they are within" the warrant's scope. 906 F.2d 841, 845 (2d Cir. 1990) (emphasis added). This principle necessarily implies that a warrant cannot authorize the seizure of suspect's papers (i.e., via removal or copying) once an officer **has examined** them and **has determined** that they do not fall within the warrant's scope. And so, guided by this principle, the Ninth Circuit in *United States v. Tamura,* condemned the government's "unconstitutional manner of executing [a] warrant" by seizing several volumes of paper documents and then keeping these volumes for "at least six months after locating the relevant documents." 694 F.2d 591, 597 (9th Cir. 1982).

The government thus has every reason to know that its continued detention of digital papers that are not responsive to a lawful warrant violates the Fourth Amendment. Certain aspects of Fourth Amendment law may, of course, merit reexamination in the digital age to ensure greater protection of personal privacy. *See, e.g.*, *Jones,* 132 S. Ct. at 957 (Sotomayor, J., concurring) (explaining why the Supreme Court should rethink the third-party disclosure doctrine in light of the digital age). But the basic rule that the government must return "items outside the scope of a valid warrant" is not one of these principles. *Matias*, 836 F.2d at 747.

3. The panel majority correctly held that the government's detention of Ganias's non-responsive digital papers was an inexcusable violation of the Fourth Amendment.

In the present case, a three-judge panel of this Court held that the government violated the Fourth Amendment by indefinitely detaining copies of a defendant's digital papers that were not responsive to a lawful warrant. *Ganias,* 755 F.3d at 137–40; *see id.* at 141 (Hall, J., concurring in part). But the panel split on whether evidence derived from this violation should be suppressed, with the panel majority favoring suppression. *See id.* at 140– 41 (majority op.); *id.* at 141–42 (Hall, J., dissenting in part).

In rehearing this case *en banc*, this Court should endorse the panel majority's holding on both the violation and suppression issues. At the same time, Amicus respectfully submits there are several aspects of the panel majority's holding that merit further consideration.

A. The government violated the Fourth Amendment by detaining Ganias's non-responsive digital papers after classifying them to be non-responsive.

The panel correctly held that the government violated the Fourth Amendment in this case. *See* 755 F.3d at 137–40; *see id.* at 141 (Hall, J., concurring in part). The government's original warrant to seize certain limited corporate financial records from Ganias's computers did not

authorize the seizure of any other digital papers. *See id* at 128. Ganias thus had every right to exclusive possession of these non-responsive papers, and the government had no authority to keep copies of these papers once it had taken the documents it was entitled to seize. *See supra* Parts I.A, I.B.

The panel's Fourth Amendment analysis leaves an open question, however, that this Court should address in its *en banc* opinion. The panel's analysis implies that what was truly problematic about the government's detention of Ganias's non-responsive digital papers in this case was the fact that this detention lasted over two-and-a-half years—an "unreasonable amount of time," in the panel's view. 755 F.3d at 137. But this raises the question: Is there some "reasonable amount of time" that the government may detain a person's papers for, even though it has already decided these papers are non-responsive to a lawful warrant? In other words, if two-and-half-years is too long, what about a year? Six months? Four weeks?

Thankfully, the Supreme Court's recent decision in *Rodriguez* (as noted in Part I.B) furnishes a bright-line answer: the police may detain persons or property for only that time period which is necessary to effectuate a lawful task. *See Rodriguez,* 135 S. Ct. at 1615. Here, that time period was 13 months, which is how long it took for the government to

locate and extract the responsive digital papers on Ganias's hard drives. 755 F.3d at 129. After that, the government was obliged to return Ganias's non-responsive papers. *See Matias*, 836 F.2d at 747. This Court should thus endorse the panel's Fourth Amendment analysis while further clarifying that the detention of Ganias's non-responsive digital papers was unlawful for **any** time period beyond the 13 months that it took the government in fact to "complete [its] mission." *Rodriguez*, 135 S. Ct. 1616.

B. The government detained Ganias's non-responsive digital papers as a matter of general practice, making the good-faith exception inapplicable.

The panel majority correctly held that the government's violation of the Fourth Amendment in this case required evidentiary suppression. *See* 755 F.3d at 140. The government kept Ganias's non-responsive digital papers long after it had determined that these papers were non-responsive, and it did so as a matter of course. *See id* at 128–29. As the agents who were responsible for the unlawful detention of Ganias's digital papers testified, they "routinely" avoided deleting non-responsive papers because "[y]ou never know what data you may need in the future." *Id.* at 129.

Given these realities, application of suppression was "especially appropriate" in this case because the Fourth Amendment violation at issue

was a direct result of the government's own routine practice—versus being the result of an isolated mistake or reliance on some external authority. *Edwards*, 666 F.3d at 886; *see also supra* Part II.A. But the panel majority did not rest its suppression analysis on this point. Instead, the panel majority emphasized its belief that "the agents here did not act good faith" insofar as these agents initially acknowledged that Ganias was entitled to the return of his non-responsive digital papers. *Id.* at 140.

Rejecting this conclusion, Judge Hall dissented, finding no bad faith in the government's detention of Ganias's non-responsive digital papers for over two years. *See id.* at 141. Judge Hall rested this conclusion largely on the following point: "[T]here was little caselaw either at the time of the search or in the following years to indicate that the Government could not hold onto the non-responsive material in the way it did." *Id.* at 142.

This reasoning should be rejected by the Court, for it encourages the police to treat digital papers as exempt from settled Fourth Amendment law. But the Fourth Amendment protects all "papers," regardless of their form. *See supra* Part I.B, II.B. This means that the government must, when possible, try to apply the lessons of settled Fourth Amendment law for physical papers to digital papers. Under this body of law, the detention of a

person's papers "after locating the relevant documents" is clearly "unconstitutional," *Tamura*, 694 F.2d at 597, and "the normal remedy is suppression and return of those items." *Matias*, 836 F.2d at 747.

With that in mind, this Court should also pivot away from the subjective "bad faith" thrust of the panel majority's suppression analysis. This is because "[t]he pertinent analysis of deterrence and culpability is objective, not an 'inquiry into the subjective awareness of arresting officers.'" *Herring*, 129 S. Ct. at 703. Suppression is therefore proper in this case not because of the subjective mental state of the officers who detained Ganias's papers but because of **the general police practice** guiding them. *See supra* Part II.A. The government was "routinely" keeping the non-responsive digital papers that it seized from suspects like Ganias in order to take future advantage of them. 755 F.3d at 129. This is just the kind of "systemic error[]" which suppression is meant to address. *Herring*, 129 S. Ct. at 704. This Court should accordingly highlight this reality.

C. The government could not cleanse its detention of Ganias's non-responsive digital papers by getting a warrant to search them.

The panel majority also correctly rejected the government's argument that no Fourth Amendment violation occurred in this case because the

government later got a new warrant to search Ganias's non-responsive digital papers. *See* 755 F.3d at 138. The panel reached this conclusion by relying upon the analogous Fourth Amendment case of *Silverthorne Lumber Co. v. United States,* in which the Supreme Court held that the government could not wrongfully seize private papers, copy them, and then try to use the copies as evidence in court. *See* 251 U.S. at 391–92.

While the panel majority's reasoning here is sound, it does leave unaddressed a significant point raised by Judge Hall in dissent: that "the Government scrupulously avoided reviewing files that it was not entitled to review before obtaining [a later] search warrant." 755 F.3d at 142. The panel majority's reasoning also elides the government's main point in its request for panel rehearing: that suppression is improper because it was the magistrate who erred in granting the government a new warrant to search Ganias's non-responsive digital papers. (*See* Gov't Pet. 7–9.)

This Court should reject the preceding points for the same basic reason: enabling the government to use the warrant process to cleanse its improper detention of a person's non-responsive digital papers subverts the crucial role of the magistrate under the Fourth Amendment. This role is "to hold the balance steady between the protection of individual privacy

on the one hand and the public need to recover evidence of wrongdoing on the other." *United States v. Travisano*, 724 F.2d 341, 345 (2d Cir. 1983).

With this in mind, while the dissent emphasizes that the government never peeked at Ganias's non-responsive papers before getting a warrant to do so, the Court must also consider "what may be" in applying the Fourth Amendment. *Weems v. United States*, 217 U.S. 349, 373 (1910). This means recognizing that a magistrate must "satisfy himself as to the adequacy and reliability of the facts set forth in the application before him." *Travisano*, 724 F.2d at 345. It also means recognizing how this crucial task is frustrated when the government is told that it may cleanse its unlawful detention of a person's digital papers through a warrant application.

This is because the magistrate cannot know with any real certainty whether the government's warrant application is tainted by an improper peek or not. If the government did peek, the application will not likely say so—even though the application itself may entirely be the product of what the government learned by peeking. By contrast, when the government applies for a warrant to search papers that are not already in its custody, the magistrate can be fairly certain that she is not granting a warrant to search papers that, in fact, have already been searched.

This analysis, in turn, discredits the government's argument that suppression is improper in this case because the government relied in good faith on a new warrant to search Ganias's non-responsive digital papers. The government emphasizes that its 2006 warrant application "made clear to the magistrate judge that the … [papers] to be searched were those retained by the government after the November 2003 seizure." (Gov't Pet. 9.) But what the 2006 application (*see* J.A. 457–72) did not make clear to the magistrate is that the papers to be searched were ones the police no longer had any right to detain, having already extracted the relevant digital papers by December 2004. 755 F.3d at 129; *see supra* Part I.C.

This ultimately is why the government's later application for a search warrant here cannot cleanse its unlawful detention of Ganias's digital papers. Presuming the magistrate in this case erred in granting the government's 2006 warrant application, this error was entirely of the government's own making. The government made no effort in its 2006 warrant application to provide the facts that would have enabled the magistrate to avoid this error. Now, "to hold the balance steady," this Court should order suppression to ensure the government does not omit such facts in the future. *Travisano*, 724 F.2d at 345.

Conclusion

Eighty-seven years ago, Justice Brandeis warned that the day might come when the government "without removing papers from secret drawers" would nevertheless be able to "reproduce them in court." *Olmstead*, 277 U.S. at 474 (Brandeis J., dissenting). That day has arrived. The government now has the power to make and keep perfect copies of every digital paper created by Americans in their homes or offices. The Fourth Amendment's protection of "papers," in turn, is meant to ensure that such power is not abused. This Court should accordingly hold that: (1) the detention of a person's digital papers beyond the time necessary to determine their responsiveness to a lawful warrant is unconstitutional; and (2) where the government has engaged in such detention as a matter of general practice, evidentiary suppression is required.

Dated: July 29, 2015

s/ *Mahesha P. Subbaraman*

Mahesha Subbaraman
SUBBARAMAN PLLC
222 S. 9th Street, Suite 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

Counsel for Amicus Curiae
Restore the Fourth, Inc.

Certificate of Compliance

The undersigned certifies under Federal Rule of Appellate Procedure 32(a)(7)(C) that this brief complies with all the applicable type-volume limitations, typeface requirements, and type-style requirements set forth under Rule 32(a). This brief was prepared using a proportionally spaced font (Book Antiqua). Exclusive of portions exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(III), this brief contains 6,677 words, according to the word-count function of the word processor (Microsoft Word 2010) that was used to prepare this brief.

Dated: July 29, 2015

s/ *Mahesha P. Subbaraman*

Mahesha Subbaraman
SUBBARAMAN PLLC
222 S. 9th Street, Suite 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

Counsel for Amicus Curiae
Restore the Fourth, Inc.

Certificate of Filing and Service

The undersigned certifies that on July 29, 2015, he caused this document—Brief of *Amicus Curiae* Restore the Fourth in Support of Defendant-Appellant Stavros Ganias—to be filed electronically with the Clerk of the Court using the CM/ECF System, which will send notice of such filing to counsel of record for all parties and *amici curiae* to this case. The undersigned further certifies that counsel of record for all parties and *amici curiae* to this case are registered as ECF Filers, and that they will accordingly be served by the CM/ECF system.

Dated: July 29, 2015

s/ *Mahesha P. Subbaraman*

Mahesha Subbaraman
SUBBARAMAN PLLC
222 S. 9th Street, Suite 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

Counsel for Amicus Curiae Restore the Fourth, Inc.