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 *AMICUS CURIAE* THE CENTER FOR CONSTITUTIONAL RIGHTS IN SUPPORT OF APPELLANT

ALAN R. FRIEDMAN
Counsel of Record
SAMANTHA V. ETTARI
NOAH HERTZ-BUNZL
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
(212) 715-9100
afriedman@kramerlevin.com

Counsel for Amicus Curiae

July 29, 2015

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, the undersigned states that none of the organizations that join this brief issues stock or has a parent corporation that issues stock.

/S/ ALAN R. FRIEDMAN
ALAN R. FRIEDMAN
Counsel of Record
SAMANTHA V. ETTARI
NOAH HERTZ-BUNZL
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
212-715-9100
afriedman@kramerlevin.com
Counsel for Amicus Curiae

July 29, 2015

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES & RULES

OTHER AUTHORITIES

STATEMENT PURSUANT TO FED. R. APP. P. 29(a) & 29(c)(5)

Pursuant to Rules 29(a) & 29(c)(5) of the Federal Rules of Appellate Procedure, the undersigned states that all parties have consented to the filing of this *amicus curiae* brief. The undersigned further states that no counsel for a party authored this brief in whole or in part, and no counsel for a party made a monetary contribution intended to fund the preparation or submission of this brief. In addition, no persons or entities other than the *amicus curiae* joining this brief, their members, or their counsel made a monetary contribution to the preparation or submission of the brief.

/S/ ALAN R. FRIEDMAN
ALAN R. FRIEDMAN
Counsel of Record
SAMANTHA V. ETTARI
NOAH HERTZ-BUNZL
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
212-715-9100
afriedman@kramerlevin.com
Counsel for Amicus Curiae

July 29, 2015

INTERESTS OF *AMICUS CURIAE*

Amicus curiae ("Amicus") the Center for Constitutional Rights ("CCR") is a national non-profit legal and educational organization dedicated to advancing and protecting the rights guaranteed by the United States Constitution and the Universal Declaration of Human Rights. Founded in 1966, CCR has a long history of litigating cases on behalf of those with the fewest protections and least access to legal resources. CCR is actively engaged in litigation representing U.S. and foreign nationals in cases implicating national security and/or allegations of terrorist activity, including *Rasul v. Bush*, 542 U.S. 466 (2004), *Boumediene v. Bush*, 553 U.S. 723 (2008), *Arar v. Ashcroft*, 585 F.3d 559 (2nd Cir. 2009) (*en banc*), and *Turkmen v. Hasty*, No. 13-981, 2015 WL 3756331 (2nd Cir. June 17, 2015). CCR has submitted amicus briefs in cases involving surveillance of electronic communications, and suspected "enemy combatants" held in military and/or criminal custody.[1] CCR has also protected the rights of marginalized political activists for over forty years and litigated historic constitutional law cases, including *Dombrowski v. Pfister*, 380 U.S. 479 (1965), *United States v. U.S. Dist. Ct. for E.D. Mich.*, 407 U.S. 297 (1972), *Texas v. Johnson*, 491 U.S. 397 (1989), and *United States v. Eichman*, 496 U.S. 310 (1990).

[1] *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013); *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004); *Rumsfeld v. Padilla*, 542 U.S. 426 (2004); *Hamdan v. Rumsfeld*, 548 U.S. 557, (2006); *Hamdan v. United States*, 696 F.3d 1238 (D.C. Cir. 2012); *United States v. Ghailani*, 751 F. Supp. 2d 515 (S.D.N.Y. 2010).

INTRODUCTION AND SUMMARY OF ARGUMENT

In *United States v. Ganias*, a panel of this Court overturned a tax evasion conviction when the Government, upon execution of a search warrant, copied the defendant's hard drives, "retained files beyond the scope of the warrant for more than two-and-a-half years" and made use of the data pursuant to a second warrant in a subsequent criminal investigation (the "2014 Panel Decision").[2] CCR respectfully submits that the 2014 Panel Decision correctly found that this conduct violated Mr. Ganias' Fourth Amendment rights.[3]

CCR submits that in executing electronic searches in which the Government seizes both responsive and nonresponsive data, the Government is required to use the responsive data only for the purposes of the originally issued warrant, adhering to the Fourth Amendment's particularity requirement, and to return and delete nonresponsive digital data after a reasonable period. Such reasonable restrictions, consistent with the panel decision, resolve this case and provide definite limitations to prevent digital searches from resembling the "general warrants" feared and rejected by the Founding Fathers.

---

[2] 755 F.3d 125, 127–30, 138 (2nd Cir. 2014), *rehearing en banc granted*, *United States v. Ganias*, Docket No. 12-240-cr, 2015 WL 3939426 (2nd Cir. June 29, 2015).

[3] This amicus brief does not address the application of the exclusionary rule and suppression.

ARGUMENT

I. A SEARCH WARRANT EXECUTED ON A COMPUTER MAY EASILY RESEMBLE OR BECOME AN IMPERMISSIBLE GENERAL SEARCH

A. A Computer May Contain Vast Amounts of Personal Data that, Even if Unresponsive, Is Collected in the Execution of a Search Warrant Reaching Electronically Stored Information

For many people, their computer hard-drive – whether in a desktop, laptop, tablet, cell phone, or some combination of the four – contains vast volumes of important personal information. This information often includes banking, finance, tax, and investment records; personal photographs, videos, and email correspondence; calendars, travel documents, and itineraries; educational, medical, and licensing records; information pointing to musical, literary, political, and religious preferences; browser, password, and search histories; word processing documents, including those that may have been deleted and abide fragmented across computer slack space; and the list goes on and on.[4] Moreover, if the device is used for work, the hard-drive may contain much or all of the same types of

[4] *See, e.g.*, Webwise, *How do I use hardware to back up my computer?*, BBC (Oct. 10, 2012), *available at* http://www.bbc.co.uk/webwise/guides/hardware-backup-solutions; Jennifer Saranow Schultz, *How to Protect Data After Laptop Theft*, N.Y. Times (Oct. 13, 2010), *available at* http://bucks.blogs.nytimes.com/2010/10/13/how-to-protect-data-after-laptop-theft/?_r=0; Charles Arthur, *Before you sell your computer, smash the hard drive, says Which?*, the Guardian (Jan. 8, 2009), *available at* http://www.theguardian.com/technology/2009/jan/08/hard-drive-security-which; Andrew Hoog, *Slack Space*, Now Secure (Oct. 17, 2008), *available at* https://www.nowsecure.com/blog/2008/10/17/slack-space/; Brian Bergstein, *There for the taking: Unprotected data make laptops a growing hazard*, N.Y. Times (July 12, 2006), *available at* http://www.nytimes.com/2006/07/12/technology/12iht-laptop.2180633.html.

information belonging to employers, clients, or third-parties. "Laptop computers are essential tools in today's global economy. Employees at all levels, in all business sectors, must be mobile," and these laptops often contain "critical information on the company, its plans, and its customers. . . ."[5] That this vast array of electronically-stored information ("ESI") is private – and should not be exposed to Government review unless falling within the clear delineations of a search warrant – is uncontroverted.

Last year, in *Riley v. California*, the Supreme Court addressed the amount of personal electronic data that individuals now amass on personal, computerized devises, when considering (and rejecting) whether mobile phones could be searched incident to arrest without a particularized search warrant.[6] Justice Roberts remarked on the storage capacity of – and nature of data contained on – cell phones:

> One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. . . . Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read. . . . The storage capacity of cellphones has several

[5] Glenn Kitteringham, *Lost Laptops = Lost Data: Measuring Costs, Managing Threats*, ASIS Foundation (2008), 3–4, *available at* www.popcenter.org/library/crisp/Laptop-theft.pdf.

[6] 134 S. Ct. 2473, 2485 (2014).

> interrelated consequences for privacy. First, 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. Second, a cellphone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.[7]

The storage capacity on cell phones – which "tend to have a lower capacity hard drive . . . and thus hold less information" – is dwarfed by that of a computer hard-drive.[8] And, while hard-drives have decreased in physical size over the decades, their storage capacity has increased exponentially.[9]

The differences between searching a premise and searching a computer are equally – if not more – dramatic than those distinguishing a cell phone and a premise. When Orin S. Kerr, a professor at George Washington University Law School and leading scholar on privacy and electronic discovery jurisprudence, authored *Searches and Seizures in a Digital World* in 2005, the difference in storage capacity between a computer and a home was already noteworthy, and, as he predicted, the magnitude of the computer's capacity continued to increase:

---

7 *Id.* at 2489.

8 Data Recovery Labs, *What is a Hard Drive?*, *available at* http://www.datarecoverylabs.com/what-is-a-hard-disk-drive.html.

9 *See* Joel Santo Domingo, *SSD vs. HDD: What's the Difference?*, PC Magazine (Feb. 17, 2015), *available at* http://www.pcmag.com/article2/0,2817,2404258,00.asp ("Capacities have grown from multiple megabytes to multiple terabytes, an increase of millions fold.").

> [An] important difference between computers and homes concerns how much they can store and how much control people have over what they contain. Homes can store anything . . . but their size tends to limit the amount of evidence they can contain. . . . Computers can only store data, but the amount of data is staggering. Computer hard drives sold in 2005 generally have storage capacities of about eighty gigabytes, roughly equivalent to forty million pages of text – about the amount of information contained in the books on one floor of a typical academic library. These figures will soon be [and now are] outdated, as computer storage capacities tend to double about every two years.[10]

With that increased storage capacity and the digitalization of nearly every aspect of human interaction, an individual's private life can often be found wholly memorialized on his or her computer hard-drive(s).[11]

B. Rule 41's Limited Exception for Large-Scale ESI Collection Should Not Swallow the Rule against General Search Warrants

Because ESI responsive to a search warrant can be massive in size, spread out or fragmented across a hard drive, obscured through misleading file names, or

---

[10] Orin S. Kerr, *Searches and Seizures in a Digital* World, 119 Harv. L. Rev. 531, 541-42 (2005).

[11] The recent allegedly Chinese state-sponsored hacks of the federal Office of Personnel Management highlight the amount of personal data that can be stored electronically. Among the data hacked were lengthy questionnaires of millions of past and present civilian employees that included "an exhaustive examination of an applicant's personal history, including their financial records (including gambling addictions and any outstanding debt), drug use, alcoholism, arrests, psychological and emotional health, foreign travel, foreign contacts, and an extensive list of all relatives." Natasha Bertrand, *We May Be Witnessing 'The Worst Breach of Personally Identifying Information Ever'*, Business Insider (June 12, 2015), *available at* http://www.businessinsider.com/level-of-damage-omp-hack-2015-6. *See also* Ellen Nakashima, *Officials: Chinese Had Access to U.S. Security Clearance Data for One Year*, Washington Post (June 18, 2015), *available at* http://www.washingtonpost.com.

hidden through overt subterfuge, Federal Criminal Procedure Rule 41 ("Rule 41") contains a limited exception that may permit the Government when applying a warrant to ESI to take digital information away from the searched premises in their entirety – usually through mirror imaging or copying – for review offsite.[12] Rule 41 provides that, specific to ESI, a warrant may, where necessary, "authorize the seizure of electronic storage media or the seizure or copying of [ESI]."[13] Unless the warrant otherwise specifies, such as by requiring, where feasible, an on-site review, the rule then "authorizes a later review of the media or information consistent with the warrant."[14] To cabin this broad collection – to ensure that the ESI exception does not swallow the particularity requirement inherent in Rule 41 – the commentary indicates that an issuing court may impose "a deadline for the return of the storage media."[15]

C. An Electronic Search is not a License for a General Warrant

This exception allowing the wholesale removal, copying, or mirror imaging of hard-drives should not be abused. Search warrants are to be as "limited as

---

12 Fed. R. Crim. P. 41(e)(2)(B).

13 *Id.*

14 *Id.* Rule 41 is problematic as it "creates a two-step procedure for the search and seizure of electronic information that necessarily allows seizing far more information than a warrant specifies." *In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 8 (D.D.C. 2013).

15 Fed. R. Crim. P. 41(e)(2)(B), Advisory Notes, 2009 Amendments, Subdivision (e)(2).

possible" and their enforcement must guard against "a general, exploratory rummaging in a person's belongings."[16] Otherwise, the danger is great that the warrant will morph into a "general warrant." Such general warrant searches are anathema under the Fourth Amendment:

> General warrants permitted the King's officials to enter private homes and conduct dragnet searches for evidence of any crime. The Framers of the Fourth Amendment wanted to make sure that the nascent federal government lacked that power. To that end, they prohibited general warrants: every search or seizure had to be reasonable, and a warrant could issue under the Fourth Amendment only if it particularly described the place to be searched and the person or thing to be seized.[17]

The risk that a warrant may manifest as a "general warrant" is particularly acute with the search and seizure of ESI. Simply because information targeted in the execution of the warrant is contained on an electronic devices or hard drive does not allow for the abandonment of these bedrock principles for limiting the way in which search warrants should be issued pursuant to the Fourth Amendment.

D. The Fourth Amendment Rejects Indefinite Possession of Non-Responsive Materials

The Government's ability to collect ESI is not unfettered or indefinite. Even pre-digital Fourth Amendment jurisprudence rejected the notion that the

---

[16] *In the Matter of the Search of Information Associated with the Facebook Account*, 21 F. Supp. 3d at 6 (citations and internal quotation marks omitted).

[17] Kerr, *Searches and Seizures*, at 536.

Government could hold physical objects indefinitely or retain copies of files when the originals were seized improperly or outside the scope of the warrant.[18] *United States v. Tamura* is instructive on this point. There, the Ninth Circuit criticized the Government's improperly broad search and seizure, including the removal off-site of documents outside the scope of the warrant, and its refusal to return the non-responsive documents.[19] "It is highly doubtful whether the wholesale seizure by the Government of documents not mentioned in the warrant comported with the requirements of the fourth amendment. As a general rule, in searches made pursuant to warrants only the specifically enumerated items may be seized."[20]

Moreover, where an overbroad search (by accident or by definition as with ESI) results in the collection of non-responsive material, it must be returned: "We likewise doubt whether the Government's refusal to return the seized documents not described in the warrant was proper. . . . The Government's unnecessary delay in returning the master volumes appears to be an unreasonable and therefore unconstitutional manner of executing the warrant."[21] These restrictions on the

---

[18] *See United States v. Place*, 462 U.S. 696, 709 (1983) (holding that a 90-minute detention of the defendant's luggage was unreasonable; "[t]he length of the detention of respondent's luggage alone precludes the conclusion that the seizure was reasonable in the absence of probable cause."); *see also Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920) (reversing judgment because government wrongfully reviewed, copied, and acquired knowledge from documents improperly seized).

[19] 694 F.2d 591 (9th Cir. 1982).

[20] *Id.* at 595.

[21] *Id.* at 596-97.

Government's retention of responsive *and* unresponsive materials are not abandoned when confronted with ESI.

II. MINIMIZATION MEASURES ARE CRITICAL FOR PROTECTING AGAINST IMPERMISSIBLY BROAD SEARCHES AND SEIZURES OF ESI

The dangers of dragnet ESI collections resulting from this expansive data collection exception have been increasingly commented upon by the courts. *In Matter of Search of Information Associated with Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, Magistrate Judge John M. Facciola, a leading jurist on civil and criminal e-discovery issues, addressed the possibility of Government "abuse" in light of the current practice of "over-seizing" when conducting an ESI search.[22] Because this over-seizing has resulted in the Governments' access "'to a larger pool of data that it has no probable cause to collect,' this Court is obligated to create minimization procedures to limit the possibility of abuse by the government."[23]

Numerous courts have responded to overbroad digital seizures with minimization measures.[24] These measures include strict applications of the Fourth

---

[22] 21 F. Supp. 3d 1, 8 (D.D.C. 2013).

[23] *Id.* (citing *United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013)).

[24] *See infra* notes 25–26. Some courts have affirmed the status quo and determined that no modifications are required. *See* James Saylor, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. 2809, 2830–32 (2011); *United States v. Mann*, 592 F.3d 779, 785–86 (7th Cir. 2010); *United States v. Williams*, 592 F.3d 511, 523 (4th Cir. 2010).

Amendment's particularity requirement, specialized search protocols to search only for information for which there is probable cause, and restrictions on Government use of nonresponsive ESI.[25] A consistent theme among these decisions is the requirement that the Government return and destroy nonresponsive ESI.[26]

---

[25] *See United States v. Galpin*, 720 F.3d 436, 446–47 (2nd Cir. 2013); *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1180 (9th Cir. 2010); *In the Matter of the Search of Information Associated with the Facebook Account*, 21 F. Supp. 3d at 10.

While some commentators have recommended a reexamination of the plain view exception in the digital context, the resolution of this issue is not necessary to resolve the facts at issue in the 2014 Panel Decision. *See Riley*, 134 S. Ct. at 2480–82; Kerr, *Searches and Seizures*, at 576–77; *Ganias*, 755 F.3d at 137–40. Commentators have suggested that the plain view exception to the Fourth Amendment is at the root of the problem of digital searches. *See* Kerr, *Searches and Seizures*, at 576–77. The plain view exception holds that police may seize evidence in plain view during a lawful search if the officer is lawfully present and has a right of access to the object, and the object's incriminating character is immediately apparent. *Williams*, 592 F.3d at 521.

This philosophy models the approach set out in *Riley v. California*, which considered the reasonableness of a warrantless search of a cell phone incident to a lawful arrest. 134 S. Ct. at 2480–82. The *Riley* Court determined that while the existing search incident to arrest "rule strikes the appropriate balance in the context of physical objects [its rationales do not have] much force with respect to the digital content on cell phones." *Id.* at 2484. The problem with the plain view exception in the digital context is that as "[m]ore and more evidence comes into plain view . . . the particularity requirement no longer functions effectively as a check on dragnet searches." Kerr, *Searches and Seizures*, at 577. However, it is possible that the meaning of plain view is itself diminished in the digital context because government review of nonrelevant data may be inevitable in the digital context, even if the exception is technically abolished. *See* Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, Texas Tech Law Review (forthcoming), 24, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2628586.

[26] *See, e.g., In the Matter of the Search of Information Associated with the Facebook Account*, 21 F. Supp. 3d at 10; *Comprehensive Drug Testing*, 621 F.3d at 1180.

The particularity requirement is a key tool.[27] Subject to this requirement, a warrant must identify the specific offense for which the police have established probable cause; describe the place to be searched; and specify the items to be seized in relation to designated crimes.[28] In *United States v. Galpin* the Second Circuit affirmed that a warrant was invalid after the police found child pornography on a suspect's computer as there was no probable cause to believe the suspect had "committed any offense beyond failing to register an internet identifier[.]"[29] The Court relied on the particularity requirement, which "'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another.'"[30] "Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance . . . [as] advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."[31]

In *United States v. Comprehensive Drug Testing*, the Ninth Circuit, *en banc*, upheld three underlying orders based on the overreach of digital searches, finding

---

[27] *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011) ("A warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity").

[28] *Galpin*, 720 F.3d at 445–46.

[29] *Id.* at 442.

[30] *Id.* at 446 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)).

[31] *Id.*

specifically that – while they recognized "the reality that over-seizing is an inherent part of the electronic search process" – the "process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect."[32]

Chief Judge Kozinski concurred separately, joined by four judges, "to provide guidance about how to deal with searches of electronically stored data in the future so that the public, the government and the courts of our circuit can be confident such searches and seizures are conducted lawfully."[33] Accordingly, Chief Judge Kozinski set out a series of key minimization measures: (1) magistrate judges must require that the government waive reliance on the plain view doctrine in digital evidence cases; (2) the segregation and redaction of nonresponsive data must be done by specialized government personnel or independent third parties; (3) warrants must disclose risks of destruction of information, as well as prior efforts to seize the information; (4) the search protocol must be designed to uncover only the information for which there is probable cause, and only this information may be examined; (5) "[t]he government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing

[32] 621 F.3d at 1177.

[33] *Id.* at 1178.

magistrate informed about when it has done so and what it has kept."[34] Additional courts have adopted these recommendations.[35]

III. THE COURT SHOULD ENDORSE THE RETURN AND DESTROY RULING OF THE 2014 PANEL DECISION

The 2014 Panel Decision correctly concluded "that the unauthorized . . . retention of . . . documents was unreasonable."[36] "Without some independent basis . . ." the Government was not permitted to retain "the files for a prolonged period of time[.]"[37] Under that rule, the Government cannot retain ESI that is not responsive to the original search warrant past a period reasonably necessary given the complexity of the original investigation.[38] The nonresponsive data should be returned, to the extent the suspect may lawfully possess it, and completely deleted (or destroyed) from Government computers.[39] In addition, the particularity requirement should be strictly construed in the digital context to ensure that the

---

34 *Id.* at 1180.

35 *See In re Search Warrant*, 193 Vt. 51, 75–93 (VT 2012) (requiring preliminary search by separate parties, prohibiting the use of sophisticated searching software, and requiring the non-retention of nonresponsive data); *In re United States' Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1152–53 (W.D. Wash. 2011) (denying search warrant for digital information that did not follow the "procedural protections [Comprehensive Drug Testing] deemed both wise and necessary[.]"

36 *Ganias*, 755 F.3d at 137.

37 *Id.* at 138.

38 *See In the Matter of the Search of Information Associated with the Facebook Account*, 21 F. Supp. 3d at 10; *Comprehensive Drug Testing*, 621 F.3d at 1180.

39 *See Comprehensive Drug Testing*, 621 F.3d at 1180.

Government only uses the responsive ESI for the original search, for which there was probable cause.[40]

In addition to *Comprehensive Drug Testing*, discussed above, other courts have recognized the utility of a return and destroy requirement. Magistrate Judge Facciola has issued Secondary Orders to warrants which "explicitly require that contents and records of electronic communications that are not relevant to an investigation must be returned or destroyed and cannot be kept by the government."[41] "This minimization procedure was intended to help strike the appropriate balance between the competing interest of the government and the requirements of the Fourth Amendment . . . ."[42] "While there has never been anything stopping the government from exceeding the scope of an otherwise valid warrant when searching a physical place, it is clearly easier to do so when the government has an identical copy of an entire hard drive or database."[43]

Whatever additional minimization measures might be optimal, the return and destroy requirement is a necessary step and straightforward and workable to

---

40 *Galpin*, 720 F.3d at 446.

41 *In the Matter of the Search of Information Associated with the Facebook Account*, 21 F. Supp. 3d at 10 (overly broad warrant application required imposition of secondary order); *see also In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at a Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1, 9 (D.D.C. 2014).

42 *In the Matter of the Search of Information Associated with the Facebook Account*, 21 F. Supp. 3d at 10.

43 *Id.*

implement. While it allows the Government initial leeway, when necessary, to search digital files, as set forth in Rule 41, it provides meaningful protections to suspects and defendants.[44] Especially in the absence of the additional minimization measures proposed by *Comprehensive Drug Testing*, the return and destroy rule is particularly necessary.[45]

Applying this standard to present case, the panel correctly determined that the Government's two-and-a-half year retention of non-responsive ESI was unreasonable.[46] The Government kept the data for multiple years, without any basis to do so, until it developed additional probable cause for a different criminal investigation in 2006.[47] Accordingly, the data was kept beyond the period necessary for the original investigation; rather, it was kept for a different investigation altogether.[48] As the Government was not permitted to retain this ESI, the only available option is to return it and destroy any copies.[49] The data may not be used for a second criminal investigation.[50]

---

[44] *See Comprehensive Drug Testing*, 621 F.3d at 1176–80.

[45] *See id.*

[46] *Ganias*, 755 F.3d at 137–38.

[47] *Id.*

[48] *See id.*

[49] *Id.* at 139–40.

[50] *See id.* In this case, had the Government not kept the data, it would not have existed as the relevant files no longer existed in the same form as when the first warrant was executed. *Id.* at 130.

Ultimately, to permit such subsequent searches would allow the encroachment of a "general warrant." "The Fourth Amendment was intended to prevent the Government from entering individuals' homes and indiscriminately seizing all their papers in the hopes of discovering evidence about previously unknown crimes . . . [y]et this is exactly what the Government claims it may do when it executes a warrant calling for the seizure of particular electronic data relevant to a different crime."[51]

As the Government's investigative tools expand with the rise of computer data, it is critically important to limit this discretion meaningfully, for such overbroad seizures of personal data also expand the significant risk that the Government will investigate not crimes, but people. As Justice Robert Jackson warned: "[t]herein is the most dangerous power of the prosecutor: that he will pick people that he thinks he should get, rather than cases that need to be prosecuted. With the law books filled with a great assortment of crimes, a prosecutor stands a fair chance of finding at least a technical violation of some act on the part of almost anyone."[52]

---

[51] *Id.* at 139–40.

[52] *Morrison v. Olson*, 487 U.S. 654, 728 (1988) (quoting Robert Jackson, Attorney General under President Franklin Roosevelt and later Supreme Court Justice).

CONCLUSION

For the foregoing reasons, Amicus CCR respectfully submits that the 2014 Panel Decision correctly concluded that defendant Ganias' Fourth Amendment rights were violated because the Government improperly retained Mr. Ganias' digital information.

Respectfully submitted,

/S/ ALAN R. FRIEDMAN
ALAN R. FRIEDMAN
Counsel of Record
SAMANTHA V. ETTARI
NOAH HERTZ-BUNZL
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
212-715-9100
afriedman@kramerlevin.com
Counsel for Amicus Curiae

July 29, 2015

CERTIFICATE OF COMPLIANCE WITH FED. R. APP. P. 29(b) & 32(a)

(1) This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) & 29(b) because this brief contains 4,461 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

(2) 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 this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman font.

/S/ ALAN R. FRIEDMAN
ALAN R. FRIEDMAN
Counsel of Record
SAMANTHA V. ETTARI
NOAH HERTZ-BUNZL
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
212-715-9100
afriedman@kramerlevin.com
Counsel for Amicus Curiae

July 29, 2015

CERTIFICATE OF SERVICE

I hereby certify that on July 29, 2015 I electronically filed the foregoing with the court's CM/ECF system, which will send notification of such filing to the counsel for all parties in these cases.

/S/ ALAN R. FRIEDMAN
ALAN R. FRIEDMAN
Counsel of Record
SAMANTHA V. ETTARI
NOAH HERTZ-BUNZL
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
212-715-9100
afriedman@kramerlevin.com
Counsel for Amicus Curiae

July 29, 2015