# 12-240

# 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**

## *AMICUS CURIAE* BRIEF OF THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF DEFENDANT-APPELLANT AND URGING REVERSAL

MARANDA E. FRITZ
ELI B. RICHLIN
THOMPSON HINE LLP
335 Madison Avenue, 12th Floor
New York, New York 10017
(212) 344-5680

RICHARD D. WILLSTATTER
GREEN & WILLSTATTER
200 Mamaroneck Avenue, Suite 605
White Plains, New York 10601
(914) 948-5656
*Vice Chair, NACDL Amicus Curiae Committee*

JOEL B. RUDIN
LAW OFFICES OF JOEL B. RUDIN, P.C.
600 Fifth Avenue, 10th Floor
New York, NY 10020
(212) 752-7600
*Vice Chair, NACDL Amicus Curiae Committee*

*Attorneys for Amicus Curiae*

## CORPORATE DISCLOSURE STATEMENT

*Amicus curiae* National Association of Criminal Defense Lawyers ("NACDL") submits the following corporate disclosure statement, as required by Fed. R. App. P. 26.1 and 29(c): NACDL is a nonprofit corporation organized under the laws of the District of Columbia. It has no parent corporation, and no publicly held corporation owns ten percent or more of its stock.

Dated: July 29, 2015
New York, New York

/s/ Maranda E. Fritz
Maranda E. Fritz

*Attorney for Amicus Curiae National Association of Criminal Defense Lawyers*

# TABLE OF CONTENTS

**Page**

# TABLE OF AUTHORITIES

**Page(s)**

**Federal Cases**

**Other Authorities**

## STATEMENT OF INTEREST

*Amicus* the National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct.[1] NACDL was founded in 1958. It has a nationwide membership of approximately 10,000 direct members in 28 countries, and 90 state, provincial and local affiliate organizations totaling up to 40,000 attorneys. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL files numerous *amicus* briefs each year in the Supreme Court and other courts seeking to provide *amicus* assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. In particular, in furtherance of NACDL's mission to safeguard fundamental constitutional rights, the Association frequently appears as *amicus curiae* in cases involving the Fourth Amendment and its state analogues, speaking to the importance of balancing core constitutional search and seizure protections with other societal interests.

[1] Pursuant to Rule 29.1 of this Court's Local Rules, *amicus curiae* certifies that (1) this brief was authored entirely by counsel for the NACDL, and not by counsel for any party, in whole or part; (2) no party and no counsel for any party contributed money to fund preparing or submitting this brief; and (3) apart from the NACDL and its counsel, no other person contributed money to fund preparing or submitting this brief.

The NACDL files this brief in support of appellant, and urges the Court to reverse the District Court decision which denied defendant Stavros Ganias's motion to suppress. The Government's prolonged retention of non-responsive documents seized from Mr. Ganias's computers amounts to a general warrant and constitutes a clear violation of the Fourth Amendment.

Based on the circumstances of this case, the particular arguments advanced by the Government on this appeal, and the conflicts that continue to arise in this Circuit concerning applications for and the execution of warrants for electronic data, the NACDL also asks this Court to address those underlying issues through a comprehensive articulation of core Fourth Amendment concepts, reinterpreted for our digital times.

## ARGUMENT

### I. THE PROHIBITION ON GENERAL WARRANTS UNDER THE FOURTH AMENDMENT BARS RETENTION OF NON-RESPONSIVE SEIZED ELECTRONIC MATERIALS

As the Supreme Court emphasized again during its 2014 term, Fourth Amendment protections played an essential role in the founding of the republic; indeed, the need to enact reforms that would provide refuge from the "general warrants" deployed by British authorities during the colonial era spurred the American Revolution itself:

> Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British

> officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." 10 Works of John Adams 247-248 (C. Adams ed. 1856). According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." Id., at 248 (quoted in Boyd v. United States, 116 U. S. 616, 625 (1886)).

Riley v. California, 134 S. Ct. 2473, 2494 (2014); see also United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013) (recognizing that "the chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants,'" quoting Payton v. New York, 445 U.S. 573 (1980)); Leonard W. Levy, Origins of the Bill of Rights 151, 157-58 (1999); Nelson B. Lasson, The History and Development of the Fourth Amendment to the United States Constitution 25-27, 79-105 (1937).

Based on that language and history of the Fourth Amendment, our courts have long articulated and enforced the limits on searches and seizures that the Government may conduct under cover of warrant. As an initial matter, no warrant may issue "unless probable cause is properly established and the scope of the authorized search is set out with particularity." Kentucky v. King, 131 S. Ct. 1849, 1856 (2011); see also Marron v. United States, 275 U.S. 192, 196 (1927) (The

particularity requirement "makes general searches . . . 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."); 2 W. LaFave, Search and Seizure § 4.6(a) (5th ed. 2012) ("[G]eneral searches are prevented by the other Fourth Amendment requirement that the place to be searched be particularly described."). Simply put, the warrant must describe with particularity the place to be searched and items to be seized, and the seizure must correspond to those specific parameters. United States v. Voustianiouk, 685 F.3d 206, 211 (2d Cir. 2012).

These time-honored principles are being stretched to a breaking point as courts, often on an *ad hoc* basis, have grappled with the proper interpretation of fundamental Fourth Amendment concepts in the context of electronic seizures. In this digital age, searches and seizures invariably involve modern electronic devices that have the capacity to store massive amounts of information about every aspect of an individual's life. Government authorities have responded by persuading courts to permit "overseizures" of vast arrays of non-responsive, often exceedingly personal documents. In this and others cases, however, the Government then fails to comply with or even denies the existence of the obligations that flow from that initial "overseizure" – obligations that, in the electronic context, are a critical component of the "execution" phase of the warrant process. The resulting

litigation has produced inconsistent judicial responses, and that in turn has formed the predicate for arguments by the Government that it acted in "good faith" because the lay of the legal landscape was unclear. This confluence of developments places ever greater stress on Fourth Amendment prohibitions on general warrants.

Much of the tension in these Fourth Amendment issues flows from the increasingly common practice of an initial "overseizure" – a practice that dates back to the Ninth Circuit's 1982 decision in United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), and had been thought to apply only in limited cases. In Tamura, FBI agents were authorized by warrant to identify and seize three discrete categories of records, but the agents instead seized volumes of material. Id. at 594-95. The court found that this seizure included "large quantities of documents that were not described in the search warrant," and recognized that such an action would usually not comport with the Fourth Amendment because "[a]s a general rule, in searches made pursuant to warrants only the specifically enumerated items may be seized. Id. at 595. The court went on to observe, however, that

> In the *comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site*, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search . . . . If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material, which should be granted by the magistrate

> issuing the warrant only where on-site sorting is infeasible and no other practical alternative exists. *The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate*.

Id. at 596-97 (emphasis added) (internal citations omitted). Under the protocol contemplated by the Tamura court, the Government could gain approval to seize caches containing both responsive and non-responsive documents, transport them off-site for searching with the "essential safeguard" of "monitor[ing] by the judgment of a neutral, detached magistrate," and then *return the non-responsive documents*. Id. at 596-97.

With the widespread proliferation of powerful computers and cell phones for business and personal use, what the Ninth Circuit predicted would be "comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site" has become commonplace, and the practice of "overseizing" has become the rule rather than the exception, with many overseizures lacking any of the appropriate magisterial "monitoring" that was initially envisioned.

It is the collision of the concept of overseizure with the virtually unlimited storage capacity of modern electronic devices that now threatens to wreak havoc on our most basic Fourth Amendment protections. Seizures and searches of modern computers and cell phones present daunting challenges precisely because they have the capacity to store vast amounts of material that may touch on the most

personal, private, and confidential subjects having nothing to do with a given warrant. The Supreme Court recognized as much in its 2014 Fourth Amendment decision Riley v. California, 134 S. Ct. at 2489-91.[2] Technological innovation allows computers to function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and they can store "millions of pages of text, thousands of pictures, or hundreds of videos." Id. at 2489. These devices become "a digital record of nearly every aspect of [users'] lives—from the mundane to the intimate." Id. at 2490 (citing Ontario v. Quon, 560 U. S. 746, 760 (2010)). The data stored on such devices is also "qualitatively different" from those contained in physical records:

> An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. . . . Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life.

Id. (citations omitted).

---

[2] The Riley case concerned a warrant-less seizure and search of a cell phone incident to an arrest, but the Court's discussion applies equally to computers; indeed, the Court recognized that "[t]he term 'cell phone' is itself misleading shorthand; *many of these devices are in fact minicomputers* that also happen to have the capacity to be used as a telephone." Id. at 2489 (emphasis added).

This Court too, and others, have observed that "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." Galpin, 720 F.3d at 446.[3]

That electronic "overseizures" place so much nonresponsive and personal information in the hands of prosecutors has been addressed by the Department of Justice in its own publications. The DOJ candidly acknowledges that "almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation." Department of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations 87 (2009) ("DOJ Computer Search Manual"), *available at* http://www.justice.gov/criminal /cybercrime/docs/ssmanual2009.pdf.

Given the massive amounts of non-responsive and personal information contained on a computer, this Court has recognized that where "the property to be

[3] See also United States v. Payton, 573 F.3d 859, 861-62 (9th Cir. 2009) ("There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (noting computer's potential "to store and intermingle a huge array of one's personal papers in a single place"); United States v. Cioffi, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009) ("The dawn of the Information Age has only heightened those [privacy] concerns. The risk of exposing intimate (and innocent) correspondence to prying eyes is magnified because computers often contain significant intermingling of relevant documents with documents that the Government has no probable cause to seize.").

searched is a computer hard drive, the particularity requirement assumes even greater importance." Galpin, 720 F.3d at 446.

> *The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous*. This threat is compounded by the nature of digital storage. Where a warrant authorizes the search of a residence, the physical dimensions of the evidence sought will naturally impose limitations on where an officer may pry: an officer could not properly look for a stolen flat-screen television by rummaging through the suspect's medicine cabinet, nor search for false tax documents by viewing the suspect's home video collection. Such limitations are largely absent in the digital realm, where the size or other outwardly visible characteristics of a file may disclose nothing about its content.

Id. at 447 (emphasis added). Accordingly, this Court mandates "a heightened sensitivity to the particularity requirement in the context of digital searches" and has expressed doubt as to the availability of the plain view exception in the case of digital searches. Id. (finding warrant facially overbroad and that officers lacked probable cause to engage in searches).

This view is reflected in a forthcoming article by Professor Orin Kerr. Orin S. Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, Texas Tech L. Rev. (forthcoming 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2628586. Prof. Kerr draws a clear distinction between "initial overseizure of nonresponsive files," which may be "reasonable because investigative necessity demands it," and "subsequent use of

nonresponsive files," which "transforms the nature of the government's interference with the owner's possessory interests." Id.

> Using nonresponsive data no longer effectuates the warrant. Instead, it takes advantage of the overseizure and subsequent search necessary to carry out the warrant to transform the warrant for specific evidence into the equivalent of a general warrant. In effect, allowing use of nonresponsive data effectively treats that data as if it had been included in the warrant. *This eliminates the role of the particularity requirement, making the warrant the equivalent of a general warrant.* Subsequent use enables every computer warrant that is narrow in theory to become general in fact. Because subsequent use renders the ongoing seizure unreasonable, use of the nonresponsive files generally violates the Fourth Amendment.

Id. (emphasis added).

## II. THE GOVERNMENT'S ACTIONS IN THIS CASE VIOLATED THE FOURTH AMENDMENT'S PROHIBITION AGAINST UNREASONABLE SEARCHES AND SEIZURES

The Government's retention of nonresponsive documents in this case, including electronic files of unrelated third parties, constitutes a violation of the Government's obligation properly to "execute" the warrant and to divest itself of that which it had no right to seize under the warrant. Those circumstances, combined with the positions taken by the Government in its briefs on this appeal, illustrate the continuing threat of "privacy violations" through "overseizure," and demonstrate the need for a clear statement by this Court on the Fourth Amendment limits that apply to government searches and seizures of electronic material at each stage of the process: application, warrant, and execution.

### A. The Government's Seizure and Search of Mr. Ganias's Computers

The Government applied on November 17, 2003 for a warrant to search the office of Mr. Ganias's accounting business. SA8; see JA430. The application consisted of an investigator's affidavit and two referenced exhibits. See JA435-451. The affidavit described an investigation principally related to two businesses, Industrial Property Management ("IPM") and American Boiler, Inc. ("American Boiler"), and stated that various accounting records relating to these businesses were located at Mr. Ganias's office. Id.

The Government's application also indicated the need to seize entire electronic storage devices, remove them to off-site environments, and, over the course of weeks to months, examine potentially *all stored data* in order to identify and segregate particular files. The affidavit recognized that not all files on the computer hard drives would be eligible for seizure under the warrant, yet conspicuously did not include any of the following:

- any description of protocols or precise key word search terms that might be used to limit the Government from reviewing *all* files contained on the hard drives;[4]

[4] The warrant authorizes the Government to perform "key word searches" but there is no indication that the application specified any precise terms the Government proposed to use. JA433-34.

- any timetable by which the forensic computer search would be completed; and
- any acknowledgement of the need to return or destroy non-responsive documents contained on the hard drives once the relevant documents had been located.

On the same day the Government filed its application, a magistrate signed the search warrant. JA430; SA8-9. The search warrant authorized a search at Mr. Ganias's office, but only authorized seizure of materials related to either IPM or American Boiler. JA431-34. Notably, the warrant included search procedure techniques, including "surveying various file 'directories' and the individual files they contain," "'opening' or cursorily reading the first few 'pages' of such files in order to determine their precise contents," "'scanning' storage areas to discover and possibly recover recently deleted files [and] for deliberately hidden files," and "performing key word searches." JA434. The warrant did not, however, include any further description of search terms, set any timetable for the forensic review or specifically direct the Government to return or destroy non-responsive documents contained on the hard drives once the relevant documents had been located.

Two days later, investigators and computer specialists began to execute the warrant by making "mirror image" copies of every file on Mr. Ganias's three computers. SA9-10; JA73, JA76, JA79. These copies included not just business

records, but Mr. Ganias's personal records and private financial documents, *along with financial records of his other clients – businesses and individuals*. JA428, JA464-65. Post-seizure review by investigators and specialists proceeded, but it was not until December 2004, 13 months post-seizure, that the Government had segregated the data potentially responsive to the search warrant. SA14-16. At this point, the Government did *not* return or destroy the non-responsive documents that had been seized, and instead determined to retain *all* files that had been collected – indefinitely. JA122-24, JA145-46. The files were thereby available in response to a warrant by IRS agents in April 2006, almost *two and a half years* after the initial seizure. SA17.

### B. The Government Continues to Maintain that it May Indefinitely Keep Non-Responsive Documents

In the briefing of this appeal, the Government continued to seek to justify indefinite retention of non-responsive documents. In in its brief opposing Mr. Ganias's appeal before the original panel of this Court, ECF No. 45, the Government argued that

- the fact that the Magistrate did not include any time restrictions on the time period for review means that "the government [may] retain computer material indefinitely and 'without temporal limitation,'" id.

30-31 (quoting United States v. Anson, 304 Fed. Appx. 1, 3 (2d Cir. 2008)[5]);

- there is no basis for a Court to "impose a time limit on the government after the fact, when the magistrate judge did not do so while approving the warrant," id.;
- a "rule requiring return or destruction of all non-responsive computer data . . . is entirely impractical," id. 34.

The positions adopted by the Government in this matter do not stand in isolation. Indeed, the DOJ Computer Search Manual echoes those stances; in the Manual, the Government opines that "court-mandated forensic protocols" are unnecessary and inappropriate (79-82) and that "prosecutors should oppose" efforts by "magistrate judges to issue warrants that impose time limits on law enforcement's examination of seized evidence" (93). Nor does the Manual specifically provide that the Government must purge or return non-responsive documents following a search.

The Government also argued to the original panel that it acted in good faith in executing the November 2003 warrant because the warrant did not set out

[5] Anson, a summary order finding a search not "untimely" where the warrant "permitted the government to retain the computers and computer related equipment without temporal limitation" is distinguishable because that warrant made clear that the entire seized computer was subject to seizure as contraband. Id.

precise protocols or time limitations and because the Government "adhered" to the warrant's terms. Opp'n 42-43. Thus, the Government, in circular fashion, employs the warrant's lack of specific direction as the basis for its argument that it acted in "good faith" when it continued to hold non-responsive material—including other clients' data—even after that material had been identified as being beyond the scope of the warrant. Id.

### C. The Particularity Requirement as Applied to Warrants to Search and Seize Electronic Materials

The guidance to date from this Court on electronic searches and seizures has consisted largely of the decision in Galpin. There, the Court emphasized the "potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive" and indicated that the plain view exception might not apply to searches of electronic materials, but the Court declined to require "specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants." Galpin, 720 F.3d at 451.[6]

[6] As for other Circuit Courts, the Ninth Circuit has not yet required that warrants contain search protocols, though a key concurring opinion in United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179-80 (9th Cir. 2010), indicates that the inclusion of such protocols can amount to a safe harbor for electronic searches. A number of Circuit Courts have, at least to this point, declined to mandate that warrants include search protocols. United States v. Evers, 669 F.3d 645, 653 (6th Cir. 2012); United States v. Stabile, 633 F.3d 219, 237 (3d Cir. 2011); United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010); United States v. Burgess, 576 F.3d 1078, 1092, 1094 (10th Cir. 2009); United States v. Cartier, 543 F.3d 442, 447-48 (8th Cir. 2008); United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007).

Since then, these issues have proliferated and the Government continues to insist that it may retain material that is unquestionably beyond the scope of the warrant. Lower courts within this Circuit have reached conflicting decisions regarding retention of non-responsive electronic documents. Compare United States v. Metter, 860 F. Supp. 2d 205 (E.D.N.Y. 2012) (Irizarry, J.) (suppressing seized data after government failed over the course of 15 months to process the seized data and retain only that which was within the scope of the warrant) with United States v. Scully, 14-CR-208 (ADS)(SIL), 2015 U.S. Dist. LEXIS 73831, *94 (E.D.N.Y. June 8, 2015) (Spatt, J.) (denying motion to suppress regarding extended retention of non-responsive documents kept "for authentication purposes"). Absent clearer guidance from this Court, the handling of overseized material will be subject to the vagaries of prosecutors and conflicting views of district courts, and individuals will continue to find their private and irrelevant documents swept up and retained indefinitely by the Government – as did Mr. Ganias in this case.

With respect to the initial phase of the warrant process, a form of search protocol is the only way to apply basic Fourth Amendment protections in the "overseizure" setting. Requiring prosecutors to articulate protocols that they will employ when searching electronically stored data is entirely consistent with the Supreme Court standard that "the scope of the authorized search [be] set out with

particularity." King, 131 S. Ct. at 1856. In traditional searches, particularity required specification of a physical location (i.e., a street address along with the office or apartment and the location within that space where materials would be found). This Court has recognized that a hard drive is "akin to a residence," and that the physical contours of locations to be searched used to ensure that the government could not enter a medicine cabinet while looking for a flat screen television. Galpin, 720 F.3d at 446. However, in the electronic context, descriptions of the geographic "place" and "location" to be searched have no meaning. A digital search requires a modernized version of those concepts of "place" and "location" to fulfill the intention of particularity that lies at the heart of the Fourth Amendment. Absent a protocol, every search is an "unbridled" rummaging through the "residence" contained on the disk or hard drive seized by the Government. Search protocols are the means by which to effectuate that traditional requirement that a warrant must define the scope of the authorized search with particularity; they are the modern counterparts of those long-standing requirements, tailored to the architecture not of a building but of an electronic storage device. In re Search of Apple iPhone, 31 F. Supp. 3d 159, 166-167 (D.D.C. 2014) (noting that "the digital world . . . is entirely different" given that "sophisticated search tools exist" that "allow the government to find specific data without having to examine every file on a hard drive or flash drive").

Based on that reasoning, a number of magistrate judges have rejected warrant applications that do not sufficiently describe the search protocols investigators will use following initial overseizures. See, e.g., United States v. Phua, Case No. 2:14-cr-00249-APG-PAL, 2015 U.S. Dist. LEXIS 37301 (D. Nev. Mar. 20, 2015); In re Cellular Tels., Case No. l4-MJ-8017-DJW, 2014 U.S. Dist. LEXIS 182165, *1 (D. Kan. Dec. 30, 2014); In re Search of Apple iPhone, 31 F. Supp. 3d 159; In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Case No. 13-MJ-8163-JPO, 2013 U.S. Dist. LEXIS 123129 (D. Kan. Aug. 27, 2013); In re Search of: 3817 W. West End, 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004); but cf. In re A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386 (S.D.N.Y. 2014) (Gorenstein, M.J.). Magistrate Judge Waxse's 2014 decision from the District of Kansas provides a helpful discussion of the concerns animating these decisions, and the degree of particularity that magistrates should require for Fourth Amendment compliance.

> [T]he court must ensure that the search warrant reflects the exact scope of the government's authority to mitigate the potential for abuse as a result of authorizing of what is, in practical effect, an unconstitutionally broad search and seizure. *Limitations must exist to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search* of office file systems and computer databases. The most efficient way for the court to ensure the

> constitutionality of the investigation is to require the government to disclose, ex ante, a proposed search protocol explaining not only how it will perform the search and ensure that it is only searching sectors or blocks of the drives that are most likely to contain the data for which there is probable cause, but also whether the target devices will be imaged in full, for how long those images will be kept, *and what will happen to data that is seized but is ultimately determined not to be within the scope of the warrant*.

In re Cellular Tels., 2014 U.S. Dist. LEXIS 182165, at *31-33.

Moreover, the level of detail in the protocols contemplated by Judge Waxse, and Magistrate Judge Facciola from the District Court for the District of Columbia, are not so onerous that they would unduly burden the Government's investigatory prerogatives.[7] See Search of Apple iPhone, 31 F. Supp. 3d at 168 (noting that the court was "not dictating that particular terms or search methods should be used" but merely requiring "a sophisticated technical explanation of how the government intends to conduct the search so that the Court may conclude that the government is making *a genuine effort to limit itself to a particularized search*").

Further, facile complaints about being locked into any given protocol should be rejected out of hand: the Government can always return for additional authorization as needed. Simply put, if the Government is determined to take

[7] Nor do appropriate protocols as described impermissibly encroach upon the Government's execution of a warrant; these protocols must simply explain the methodology for determining how a search may be cabined to prevent it from becoming a general warrant. Cf. Dalia v. United States, 441 U.S. 238, 257-58 (1979) (warrant authorizing surveillance did not need to specify that bug would planted surreptitiously, as Fourth Amendment does not require warrant to "set forth precisely the procedures to be followed by the executing officers").

electronic material by search warrant (as opposed to alternative methods such as subpoena), it seems not too much to expect that they would have thought through the warrant execution process in advance such that they can include it in the warrant application. See Comprehensive Drug Testing, 621 F.3d at 1179-80 (former Chief Judge Kozinski writing in concurring opinion that "the warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown").

**D. Retention of Non-Responsive Documents**

Courts have articulated increasing concern regarding the length of time that the Government may retain non-responsive, private and confidential information contained in computers or other electronic storage devices that the Government has "overseized." A handful of lower courts in this Circuit have addressed the topic and reached, in some instances, conflicting results;[8] this Court has yet to provide

[8] The courts in Metter, 860 F. Supp. 2d 205 and Doane v. United States, 08 Mag. 0017 (HBP), 2009 U.S. Dist. LEXIS 61908, *25-30 (S.D.N.Y. June 1, 2009) (Pitman, M.J.) found extended retention impermissible. See also Carpenter v. Koskinen, No. 3:13-cv-563 (SRU), 2015 U.S. Dist. LEXIS 72075, *17 (D. Conn. June 4, 2015) (Underhill, J.) (finding that the Government may not retain indefinitely non-responsive documents "as part of a long-term fishing expedition"). The court in Scully, 2015 U.S. Dist. LEXIS 73831, *94, denied suppression where non-responsive documents were "retained for authentication purposes only." See also Google, Inc., 33 F. Supp. 3d at 399 (declining to impose any restrictions on retention in warrant).

definitive guidance on Fourth Amendment constraints in this context, and this case provides a needed opportunity for it to do so.[9]

Beyond this Circuit, a number of magistrate judges have already begun to incorporate baseline limitations within warrants to search electronic materials. This includes limiting the timeframe for the Government to conduct an electronic search. See United States v. Mutschelknaus, 592 F.3d 826 (8th Cir. 2010) (discussing sixty-day window set by magistrate for post-seizure offsite search of computers); United States v. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999) (warrant required forensic analysis within thirty days of the physical search; court suppressed files discovered through search outside of authorized time window), *aff'd*, 256 F.3d 14 (1st Cir. 2001).

Within the Circuit, the decision of Southern District Magistrate Judge Pitman provides a pertinent useful review of the relevant authorities in the context of an overseizure and ongoing retention of documents not covered by a search warrant. Doane, 2009 U.S. Dist. LEXIS 61908, *25-30. The court reviewed the applicable authority and held that "these cases *do not contemplate the indefinite retention of all materials contained within intermingled files*." Id. at *28. "[E]ven where practical considerations permit the Government to seize items that are beyond the scope of the warrant, once the fruits of the search are segregated into

[9] Indeed, over the past year the Court's original panel decision in this matter has been often cited by courts within the Circuit and elsewhere.

responsive and non-responsive groups, the 'normal' practice is to return the non-responsive items." Id. at *28. The court concluded that "permitting the Government to retain items outside the scope of the warrant without such a showing would dramatically dilute the right to privacy in one's personal papers." Id. at *30 (citing Andresen v. Maryland, 427 U.S. 463, 482 (1976)).

Far from indefinite retention, many courts have recognized that, under the Fourth Amendment, the Government is obligated to conduct the off-site forensic analysis of seized electronic equipment "within a reasonable time" and divest itself of that which is not within the scope of the warrant. United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1077 (D.N.D. 2008); see also United States v. Graziano, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008) (emphasizing that "the manner of the execution of the warrant in searching the computer will also be subject to judicial review under a reasonableness standard"); United States v. Soliman, 06-CR-236, 2008 U.S. Dist. LEXIS 87304, at *1-2 (W.D.N.Y. Oct. 29, 2008) (ordering that "items outside of the scope of the search warrant should be identified and returned to defendant"); DOJ Computer Search Manual 92 ("The Fourth Amendment does require that forensic analysis of a computer be conducted within a reasonable time.")[10] For instance, in United States v. Debbi, 244 F. Supp.

[10] Even in the Ninth Circuit's Tamura decision, the court evinced "doubt" that "the Government's refusal to return the seized documents not described in the warrant was proper." 694 F.2d at 596-97 (unreasonable for Government to keep "master

2d 235, 237 (S.D.N.Y. 2003) (Rakoff, J.), Government agents seized, pursuant to a warrant, electronic and paper files including financial and patient records, but the Government then failed to make "any meaningful attempt . . . to separate from what was actually seized the only items that the warrant permitted to be seized." Id. at 237-38. Even after the court had encouraged the Government "to do the necessary sifting and return what was, by any measure, improperly seized," the Government did not do so, "– as if, on any possible rationale, the Government would not be required to return what exceeded the plain limitation language of the warrant." Id. at 238.

> It is thus evident that the Government chose to blatantly disregard the very limitations that saved the warrant from overbreadth, and that the Government continues to do so. For all its protestations of good faith, the Government felt free to invade Debbi's home, seize his records without meaningful limitation and restraint, pick over them for months thereafter without determining which were actually evidence of the alleged crimes, *and even now refrain from returning what it was never entitled to seize*.

---

volumes" containing non-responsive documents "for at least six months *after* locating the relevant documents").

Tamura also rejected concerns, similar to those the Government raised here, about problems the Government might have authenticating evidence following the return of non-responsive documents, noting that "the testimony of the agents who removed the documents" from the full set "would have sufficed" for the purpose of authentication. Id. at 597.

Id. (emphasis added). Based on that record, Judge Rakoff suppressed all seized materials that the Government had not yet determined to be within the scope of the warrant. Id. at 238-39.

Similarly, the court in Metter addressed the "reasonableness" of the government's post-seizure conduct. 860 F. Supp. 2d 205. In Metter, the particularity and initial seizure procedures were not at issue because the warrant application properly described the allegations, the particular categories of information sought and how it related to the allegations, and the need for off-site processing. Instead, the issue in Metter arose from the government's failure to process the seized data and retain only that which was within the scope of the warrant. The court concluded that 15 months of inactivity after seizing electronic data was plainly unreasonable. Based on all of the circumstances relating to that seizure, including the Government's repeated failures to process the data, the Court held that the appropriate remedy was suppression.

To take another example from outside the Circuit, in United States v. Collins, Case No. CR 11-00471 DLJ (PSG), 2012 U.S. Dist. LEXIS 111583 (N.D. Cal. Aug. 8, 2012), the Government executed 27 search warrants and seized over 100 computers and other digital devices. Almost one year later, none of the data had been returned and the defendants submitted a motion for the Government to return all devices and non-targeted data. Id. at *19. Primarily relying on language

in the warrant, the Government argued (1) that it was permitted to retain seized devices as instrumentalities of the crime, (2) that it could retain a complete copy of the devices to link them to the defendants and to prevent impeachment of its forensic process, and (3) that it satisfied its obligation to return all data by providing complete forensic images to the defendants' discovery coordinator. The court recognized that the Government's theory would permit the seizure of storage devices without ever needing to return the data contained therein and rejected this argument. Id. at *3.

> More fundamentally, the government's argument proves too much. If separating non-targeted data from targeted data and devices lawfully retained as criminal instrumentalities is too hard here, it presumably is too hard everywhere. *In what case where a storage device is seized lawfully could a defendant or other subject of a search warrant ever secure return of data that the government had no right to take?* Just about every storage device can be searched more easily with automated scripts than manually. Just about every storage device has non-targeted data that might prove useful to understanding the data that was targeted. Just about every storage device has deleted files in unallocated space. *If the government's argument were accepted here, so that it need not return even one bit of data that is clearly outside the scope of the warrant, the court thus would render a nullity the government's pledge in just about every search warrant application it files in this district that it will return data that it simply has no right to seize*.

Id. at *4-5 (emphasis added).

### E. The Government's Violations of Mr. Ganias's Fourth Amendment Rights

Here, the Government seized all of the files on Mr. Ganias's computers pursuant to a warrant that authorized seizure only of documents concerning two

businesses. Following that initial overseizure, and 13 months of work to identify files encompassed by the warrant, the Government continued to keep documents that no warrant authorized them to hold.

Under the standards discussed above, the application and search warrant needed to describe the bounds of a *particularized* search; in the context of an electronic search, this required documenting (a) the means by which the Government would limit its access to non-responsive documents immediately following initial overseizure through established search protocols, and (b) the obligation to return or destroy non-responsive documents following a forensic search. The absence of these features render the application and warrant defective.

Further, the Government has no basis to claim that its failure to complete the execution of the warrant should be shielded by the "good faith exception." The non-responsive documents swept up with the Government's overseizure of Mr. Ganias's computers and retained indefinitely included third-party documents bearing no relation to the businesses under investigation. The reason proffered by Government agents for keeping this non-responsive information—that they considered it "the Government's property," JA146—is at the least misguided and should be rejected roundly, and underscores yet again the need for a definitive statement from this Court that one's private electronic files do not become the

"Government's property," and can only be kept by the Government if within the scope of a judicially authorized seizure.

## CONCLUSION

Under the authorities described above, the Government's seizure and indefinite retention of Mr. Ganias's files transformed a limited warrant into a forbidden general warrant and thereby violated the Fourth Amendment. Even with the benefit of time to reflect upon its execution of the warrant here, the Government continues to press this Court to ratify indefinite retention of non-responsive materials to the further erosion of Fourth Amendment protections. This Court should, in plainest terms, reject that position and reiterate the arguably self-evident proposition that a warrant permits retention only of material that is within its scope.

We are now firmly ensconced in the digital age. As modern technology becomes ever more ubiquitous and multi-functional, and as storage capacities on personal devices continue to increase, the issue of how the Government must treat intermingled electronic documents when executing a search warrant will only grow more acute. The *ad hoc* approach to date leaves the Fourth Amendment vulnerable to continued erosion, allows the Government to continue claiming that it can retain non-responsive documents "without temporal limitation," and generates avoidable litigation. And permitting the Government to rifle through and retain confidential

non-responsive electronic documents amounts to the modern equivalent of allowing "officers to rummage through homes" – the precise practice that was so abhorrent to the Founding Fathers. Riley, 134 S. Ct. at 2494. We ask that the Court take this opportunity to ensure that fundamental Fourth Amendment rights are safeguarded, notwithstanding the fact that our private documents and intimate communications now reside in compact containers that the Government can so easily copy and store.

For the reasons discussed above, we respectfully request that the Court find that the Government's actions violated the Fourth Amendment and reverse the decision in the lower court.

Dated: July 29, 2015
New York, New York

Respectfully Submitted,

/s/ Maranda E. Fritz

Maranda E. Fritz
Eli B. Richlin
Thompson Hine LLP
335 Madison Avenue
New York, New York 10017
(212) 344-5680

Richard D. Willstatter
Green & Willstatter
200 Mamaroneck Avenue, Suite 605
White Plains, New York 10601
(914) 948-5656

Joel B. Rudin
Law Offices of Joel B. Rudin, P.C.
600 Fifth Avenue, 10th Floor
New York, NY 10020
(212) 752-7600

*Attorneys for Amicus Curiae National Association of Criminal Defense Lawyers*

## CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I hereby certify that this brief complies with the type-volume limitations of Fed. R. App. P. 32(a) because it was produced using Times New Roman typeface in 14-point font and contains 6,892 words, excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii), according to the word processing system utilized by my firm.

Dated: July 29, 2015
New York, New York

/s/ Eli B. Richlin
Eli B. Richlin

**CERTIFICATE OF SERVICE**

I HEREBY CERTIFY that on this date a copy of the foregoing was filed electronically with the Court's CM/ECF system. Notice of this filing will be sent by email to the counsel for all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's CM/ECF System.

Dated: July 29, 2015
New York, New York

/s/ Eli B. Richlin
Eli B. Richlin