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

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF APPELLANT AND URGING AFFIRMANCE

Marc Rotenberg
Counsel of Record
Alan Butler
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

July 29, 2015

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c) for Case No. 13-422 *amicus curiae* Electronic Privacy Information Center ("EPIC") states that it is a District of Columbia corporation with no parent corporation or publicly-held company with a 10 percent or greater ownership interest. EPIC is a non-profit, non-partisan corporation, organized under section 501(c)(3) of the Internal Revenue Code.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. The EPIC Advisory Board includes renowned legal scholars and technology experts. EPIC maintains one of the top websites on privacy in the world, www.epic.org. EPIC routinely participates as *amicus curiae* in significant privacy cases concerning Fourth Amendment rights. *See, e.g., Riley v. California*, 134 S. Ct. 2473 (2014); *Florida v. Jardines*, 133 S. Ct. 1409 (2013); *Maryland v. King*, 133 S. Ct. 1 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012).

EPIC has a longstanding interest in preserving strong data minimization standards and preventing the erosion of privacy rights amidst technological evolution. EPIC has argued that federal courts should broadly adopt the rules set out by the Ninth Circuit in *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010), to limit the collection and retention of non-pertinent data

[1] The parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

during searches of electronic evidence. *See* Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) and Legal Scholars and Technical Experts in Support of Respondents, *Quon v. City of Ontario, CA*, 560 U.S. 746 (2010).

SUMMARY OF THE ARGUMENT[2]

The traditional rules for executing searches and seizures of physical property are insufficient to protect the privacy interests of individuals whose information is now stored on digital devices. The intermingling of records and information subject to search warrants with records that contain sensitive and otherwise irrelevant information is becoming the rule rather than the exception. In addition, the law enforcement practice of creating mirror image copies of digital files makes it significantly easier for the government to retain vast amounts of sensitive, non-pertinent records that were traditionally destroyed or returned to the owner's possession. Courts have also not yet established clear rules limiting the application of the "plain view" doctrine to files stored in hard drives and other digital repositories. The rules set out in *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, J., concurring), addressed this problem.

Sensitive personal information should not be subject to government inspection and indefinite retention merely because it happens to exist on the same

[2] EPIC would like to thank its IPIOP Summer Clerks for their help in preparing this amicus brief: Kasey Wang, Eogan Hickey, Michele Trichler, John Davisson, and Britney Littles.

storage device as a record subject to a search warrant. This exceeds the permissible scope of the government's authority to search and is an artifact of the courts' failure to make clear the boundaries of a lawful search. Unless the courts address this problem, it will get worse. The exposure of sensitive data will increase as personal devices and cloud services generate and store larger and larger volumes of data. The Court should act now to establish clear obligations to delete non-pertinent data and minimize sensitive information stored on personal devices. These principles, previously established by Congress in the Wiretap Act, 18 U.S.C. § 2518, have already been embraced by other federal courts.

ARGUMENT

It can no longer be said that it is only in "comparatively rare" instances that documents subject to a search warrant will be "so intermingled that they cannot feasibly be sorted on site." *See United States v. Tamura*, 694 F.2d 591, 595–97 (9th Cir. 1982). Today it would be surprising if a target document was not stored digitally amongst thousands of other records, and the processing of these records implicates significant privacy issues. The Court in this case is presented with the opportunity to provide guidance for lower courts and magistrates who oversee and direct the execution of search warrants for digital records.

The Ninth Circuit previously addressed this important issue in *United States v. Comprehensive Drug Testing*, 621 F.3d 1152 (9th Cir. 2010), and Judge

Kozinski's concurring opinion, joined by four other circuit judges, outlined clear rules to guide future decisions. *Id*. at 1180 (Kozinski, J., concurring). The Court should endorse these principals to ensure that digital searches do not result in indefinite storage of non-pertinent documents in law enforcement databases. As the Supreme Court recently recognized in *Riley v. California*, 134 S. Ct. 2473 (2014), digital searches implicate greater privacy interests than traditional physical files, and should be subject to increased constitutional protections. As Justice Sandra Day O'Connor earlier explained, "The police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities." *Arizona v. Evans*, 514 U.S. 1, 17 (1995) (O'Connor, J., concurring).

I. Digital Storage Devices Contain Increasingly Large Volumes of Sensitive Personal Data, Requiring Additional Restrictions on Digital Searches and Seizures

There are two trends, in particular, that have created the need for new guidelines governing the handling of search warrant returns. First, the explosion in digital storage capacity over the last several decades has made the storage of all files in electronic form commonplace. Second, the development and increasing use of cloud-based storage services has created vast repositories of intermingled data. As a result of these trends, documents subject to search warrants will increasingly

be stored on drives and servers that include thousands of intermingled and non-pertinent files. Given the sensitive nature of files stored on these digital devices—including financial records, medical records, photographs, and other personal information—it is critical that the Court establish rules ensuring that any data not subject to a valid search warrant be promptly deleted or returned to its owner.

Professor Jerry Kang has stressed that, "When the science changes—when the facts change—the law has an obligation to respond in kind, or at least tell us why it cannot." Jerry Kang, Lecture at University of Washington: The Arc of Intent: How Psychological Science Should Inform The Law (Feb. 18, 2015).[3] *See also* Julie E. Cohen, *What Privacy is For*, 126 Harv. L. Rev. 1904, 1933 (2013) (emphasizing that "Imbuing our networked information technologies with a different politics will require both the vision to appreciate privacy's dynamism and the will to think creatively about preserving it"). As Former MIT President Jerome Wiesner famously explained, legal safeguards must be established to preserve privacy rights because technological measures themselves will not be sufficient:

> There are those who hope new technology can redress these invasions of personal autonomy that information technology now makes possible, but I don't share this hope. To be sure, it is possible and desirable to provide technical safeguards against unauthorized access. It is even conceivable that computers could be programmed to have their memories fade with time and to eliminate specific identity. Such safeguards are highly desirable, but the basic safeguards cannot be

[3] *Available at* https://www.youtube.com/watch?t=502&v=dMVc1n599vg

> provided by new inventions. They must be provided by the legislative and legal systems of this country. We must face the need to provide adequate guarantees for individual privacy.

Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the House Comm. on the Judiciary, 92d Cong., 1st Sess. Part I, 761–74 (1971) (testimony of Jerome B. Wiesner, provost elect, Massachusetts Institute of Technology).

Over the last forty years, digital storage has shifted from a scarce and expensive luxury to an abundant resource. For example, in the mid 1970s a state-of-the-art 5¼-inch inch floppy disk drive held 8,000 kilobytes and cost more than $500. *In re Certain Double-Sided Floppy Disk Drives & Components Thereof at 230–32*, Inv. No. 337-TA-215, USITC Pub. 1860 (May. 1986). Today companies produce memory products that can store one hundred and twenty eight gigabytes of data on an eleven-by-ten-millimeter chip, *See* Press Release, Toshiba Offers World's Smallest-Class E-Mmc Embedded Nand Flash Memory Products (Oct. 1, 2014),[4] and hard drive disks that can store eight terabytes of data, *see* Press Release, Seagate Ships World's First 8TB Hard Drives (Aug. 26, 2014).[5]

[4] http://www.toshiba.com/taec/news/press_releases/2014/memy_14_725.jsp.

[5] http://www.seagate.com/about/newsroom/press-releases/Seagate-ships-worlds-first-8TB-hard-drives-pr-master/.

A hard drive today could hold more than a million copies of the data stored on a 5¼-inch floppy disk.[6] But even as digital storage capacity has expanded exponentially, our desire to create and store data has more than grown to meet that demand. A recent report estimates that by 2020 there will be "nearly as many digital bits as there are stars in the universe," and that the volume of stored data is currently "doubling in size every two years." Int'l Data Corp., *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things—Executive Summary* (2014).[7] The report estimates that the amount of digital data created will increase by a factor of ten by 2020, from 4.4 trillion gigabytes to 44 trillion. *Id*. Over the last few months alone, companies shipped 28.3 exabytes of storage capacity (an exabyte is "one quintillion bytes or a one followed by 18 zeros"). Lucas Mearian, *Server Sales Lead to Increased Internal Storage Growth*, Computerworld (June 30, 2015).[8]

As storage costs have decreased and users have embraced mobile devices, cloud-based email has become commonplace. The largest telecommunications providers, including Google and Microsoft, already offer cloud-based

---

[6] There are 1,073,741,824 kilobytes in a terabyte, so an eight terabyte hard drive is roughly 1,073,742 times the size of a 8,000 kilobyte floppy disk.
[7] http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.
[8] http://www.computerworld.com/article/2942045/data-storage-solutions/more-than-28-billion-gigabytes-of-storage-shipped-last-quarter.html.

communications services. These services are being used by individuals as well as large institutions such as universities, government agencies, and businesses. These large repositories of stored files and messages will necessarily include documents that will be the subject of investigations by law enforcement agents, and the processing of those databases will implicate the privacy rights of all users.

Federal agencies have been using cloud-based systems since 2010. Steve Hoffman, U.S. Gen. Servs. Admin., No. 10694, *GSA Becomes First Federal Agency to Move Email to the Cloud Agencywide* (Dec. 1, 2010).[9] Government entities in 45 states already use cloud-based services, *see* Google, *Governments in 45 States Have Gone Google* (2015),[10] and other federal, state, and local entities such as the City of Chicago, the Environmental Protection Agency, and the Federal Aviation Administration have transitioned to similar services, *see*, *e.g.*, Angela Moscaritolo, *Chicago Moving Employee Email, Apps to Microsoft Cloud*, PC Magazine (Jan. 4, 2013);[11] Josh Henretig, *EPA Migrating to Microsoft Cloud*, Microsoft Green Blog (Oct. 31, 2012).[12]

The use of cloud-based services has grown rapidly in the business sector. By 2016 an estimated eighty percent of the top two thousand businesses globally will

[9] *Available at* http://www.gsa.gov/portal/content/208417.
[10] https://www.google.com/work/apps/government/customers.html.
[11] http://www.pcmag.com/article2/0,2817,2413870,00.asp.
[12] http://blogs.msdn.com/b/microsoft-green/archive/2012/10/31/epa-migrating-to-microsoft-cloud.aspx.

have at least half of their IT infrastructure in the cloud. Int'l Data Corp., *Sharpening the Small Business Competitive Edge: Is the Time Right for the Cloud* 5 (2014).[13] Already more than eighty percent of U.S. companies with more than one hundred employees use cloud services. *Id*. And during the five-year period between 2013 and 2018 small and midsize businesses are predicted to spend twenty-eight percent of their total IT budgets (nearly one trillion dollars) on cloud services. *Id*. at 4. *See also* Franklin Morris, *Infographic: The State of SMB Cloud Adoption in 2014* (Oct. 22, 2014).[14] As businesses increasingly adopt cloud-based services, larger and larger volumes of sensitive records will be intermingled in remote data centers.

There are already over two and a half billion e-mail users worldwide, and most consumers access and store their messages through cloud service providers. The Radicati Group, Inc., *Email Market, 2014-2018: Executive Summary*, at 3–4 (2014).[15] The largest e-mail providers offer virtually unlimited storage and encourage users to retain messages rather than delete them. *See* David Eitelbach, *Yahoo Mail v. Outlook.com v. Gmail v. AOL Mail*, Laptop Mag (Sept. 19, 2014)

---

[13] *Available at* http://sapnews195twk.wpengine.netdna-cdn.com/wp-content/blogs.dir/1/files/InfoBrief_SAP-Cloud-Small-Biz.pdf.
[14] http://www.rackspace.com/blog/infographic-the-state-of-smb-cloud-adoption-in-2014/.
[15] *Available at* http://www.radicati.com/wp/wp-content/uploads/2014/10/Email-Market-2014-2018-Executive-Summary.pdf.

(AOL provides more than 150GB, Microsoft provides more than 5GB, Gmail provides 15GB, and Yahoo provides 1TB).[16] Indeed, these companies compete against each other to provide the most storage on the market. *Id*. Users no longer need to delete messages in order to preserve storage space; most messages can be retained by default. As a result, a wealth of personal and private messages are now stored remotely in intermingled databases. This means that a search of any given e-mail database could implicate the privacy interests of thousands or even millions of e-mail users.

In addition to e-mail services, many consumers store and access their documents and other sensitive files online. Erin Griffith, *Who's Winning the Cloud Storage Wars*, Fortune (Nov. 6, 2014).[17] Given the widespread use of these digital storage services, and the growth in storage capacity of individual computers and devices, the problem of searching and seizing large volumes of data will continue to increase over time. This Court should establish clear guidelines governing these digital searches going forward.

[16] http://blog.laptopmag.com/best-free-email-service.
[17] http://fortune.com/2014/11/06/dropbox-google-drive-microsoft-onedrive/.

II. The Supreme Court Established in *Riley v. California* That Searches of Digital Devices Require Additional Privacy Protections

A. The Court Explained in *Riley* That Digital Devices Are Meaningfully Different From Their Analog Counterparts

In *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court held that the traditional rule permitting searches of physical items on a suspect incident to arrest could not be extended to searches of digital devices. *Id*. at 2494–95. In reaching that conclusion, the Court focused on the unique nature of electronic devices and digital data and concluded that the intrusiveness of a search of digital data was significantly different from searches of physical objects. *Id*. at 2489.

The majority opinion in *Riley*, issued by Chief Justice Roberts, outlined key distinctions that justify special rules governing searches of digital data. First, the large quantity of information created and stored by digital devices; second, the uniquely sensitive qualities of digital records; and third, the ease with which digital data can be accessed, copied, and stored by government. These factors provide not only a basis to modify the search-incident-to-arrest rule, as the Court did in *Riley*, but also to impose greater restrictions on post-search minimization and retention of seized files.

As the Court explained in *Riley*, prior to the development of mobile computing devices "a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Id.* at

2489. With cell phones the "possible intrusion on privacy is not physically limited in the same way." *Id*. The Court found that these devices collect "in one place many distinct types of information," creating an "element of pervasiveness that characterizes" digital devices and is distinct from physical records. *Id.* at 2490. The Court emphasized that "[a]llowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case." *Id*.

These same quantitative distinctions must also apply to other forms of digital records, including mirror-image copies of files stored on a hard drive. Indeed, the amount of personal information stored on computer hard drives is vastly larger than the amount of data stored on a mobile phone. For example, a standard desktop computer purchased from Dell today includes two terabytes of storage. Dell, *Inspiron Small Desktop 3000 Series* (2015).[18] Most cell phones store less than 100 gigabytes of data.[19] It is estimated that an average desktop could store every message ever sent on Twitter. Bruce Schneier, *Data And Goliath* 18 (W.W. Norton & Company Inc. 2015).

---

[18] http://www.dell.com/us/p/inspiron-3647-small-desktop/pd?oc=ddcwnp325s&model_id=inspiron-3647-small-desktop (Last visited, July 24, 2015).

[19] A terabyte is equivalent to 1024 gigabytes of data. Understanding File Sizes, http://www.gn.apc.org/support/understanding-file-sizes (Last visited, July 24, 2015). A single five-page document usually contains approximately 30 kilobytes.

In other words, computers have inconceivable storage capabilities and most individuals routinely create and maintain large volumes of personal information—even more "pervasive" than the data stored on cell phones. As such, there is an enormous quantitative distinction between a seizure of a filing cabinet or other physical document set and the seizure of a hard drive.

The Court in *Riley* further distinguished digital searches based on the fact that the data stored on these devices is fundamentally different from the types of physical evidence traditionally subject to search. As an example, the Court cited "Internet search and browsing history" as well as location data and other sensitive information. *Riley,* 134 S. Ct. at 2490. These records can also reveal sensitive personal details including political affiliation; addiction; budgetary information; romantic life; hobbies and pastimes; and banking and financial details. *Id*.

The same types of sensitive data that the Court focused on in *Riley* are also stored on hard drives and in cloud-based services. Individuals may have saved on their hard drive detailed financial records dating back many years. They may have saved correspondence with employers, doctors, or lawyers. They may have information about their family or their future plans. Indeed, many individuals may have stored more information than they realize. As Bruce Schneier has explained, computers "sense and record more than you're aware of." Schneier, *supra* at 13.

New technological developments will lead to the creation and storage of ever more sensitive information about our daily activities. *Id*. at 15. The "Internet of Things" (IoT), a series of appliances designed to "connect [devices] and people through the existing Internet infrastructure," will result in even more data being generated by routine daily activities. *See* EPIC, *Internet of Things (IoT)*, https://epic.org/privacy/internet/iot/ (2015). Now medical devices, thermostats, fitness-tracking devices, refrigerators, cars, and many other devices are creating digital paper trails that could potentially be subject to search. Schneier, *supra* at 14–17. This produces a plethora of very diverse and detailed types of information, and much of it is saved on users' personal digital devices, including their hard drives. *Id*. at 128.

As Schneier notes, "having conversations that disappear as soon as they occur is a social norm that allows us to be more relaxed and comfortable, and to say things we might not say if a tape recorder were running." *Id*. In effect, individuals might be said to now carry a tape recorder, tracking device, and many more recorders of personal information around with them wherever they go. But just because these records are created and stored together in centralized repositories does not mean that they can be searched or indefinitely seized simply because they are on the same drive as the target document in an investigation.

As Chief Justice Roberts recognized in *Riley*, the search of the entire contents of a digital device "would typically expose to the government far more than the most exhaustive search of a house" because these devices "not only contai[n] in digital form many sensitive records previously found in the home; [they] also contain[n] a broad array of private information never found in a home in any form." *Riley*, 134 S. Ct. at 2491.

Finally, as the Court explained in *Riley*, the search of a digital device is fundamentally different because the storage and analysis of digital data is much less expensive and less time consuming for law enforcement. For the effort of a "search in the pre-digital era [that] could have turned up a photograph or two in a wallet," the search of a digital gallery would turn up "thousands of photos." *Id*. at 2942. And whereas it might have been justified to allow the officers in *Tamura* six months to search and segregate non-pertinent information from physical files, the government should not be allowed to hold onto irrelevant digital data for long periods of time. Strong rules are necessary to avoid the indefinite collection of search warrant files in government databases. Unlike with the physical files, the officers will not notice digital bits filling up the file room.

In fact, in the present case, the government accessed the information with relative ease and was capable of making copies of the data in its entirety, whether relevant to its investigation or not, to be stored permanently—all of which would

have been far more difficult, if not impossible, had the records been contained in physical files. The length of time these documents were held and the manner in which the search was carried out demonstrates the need for a "data expiration" rule. Eventually data becomes irrelevant and should be recognized as such. As Schneier points out:

> One fourth of American adults have criminal records. Even minor infractions can follow people forever and have a huge impact on their lives—this is why many governments have a process for expunging criminal records after some time has passed. Losing the ephemeral will mean that everything you say or do will be associated with you forever.

Schneier, *supra* at 128.

Prior to the development and use of electronic storage, the government simply could not have copied, searched, and stored any such amount of data with such a degree of ease. This increase in the government's ability to access large quantities of sensitive data calls for the adoption of minimization principles, including "data expiration"—in other words, that all data should have standard, pre-set durations (this is not the norm)—which many prominent scholars have been promoting for years. *See* Jeff Jonas, *Surveillance Society and Transparent You*, *in Privacy in the Modern Age: The Search for Solutions* 101 (Marc Rotenberg et al. eds., The New Press, 2015).

The Court's decision in *Riley* makes clear that digital searches are fundamentally different and require special rules to protect against the exposure of sensitive information.

III. The *Comprehensive Drug Testing* Framework Should be Broadly Applied

In *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, J., concurring), Judge Kozinski outlined specific data minimization requirements to guide magistrates in overseeing electronic data searches by law enforcement officers. This framework established a strong set of principles that allows the government to pursue appropriate investigations while ensuring that access to electronic data does not become unbounded. This framework should be applied in this and other similar cases involving searches and seizures of hard drives, which contain large volumes of sensitive personal data.

The framework outlined in *Comprehensive Drug Testing* is also rooted in the structure of the Wiretap Act, which was enacted by Congress following the Supreme Court's decisions in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967). *See Riley v. California*, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring) (reviewing the legislative history of Title III). Specifically, the rules outlined in 18 U.S.C. § 2518 address the constitutional particularity requirements articulated in *Berger*. *See United States v. Torres*, 751 F.3d 875, 883–84 (7th Cir. 1984) (explaining how the rules "safeguard against

electronic surveillance that picks up more information than is strictly necessary and so violates the Fourth Amendment's requirement of particular description"). These rules require a judge authorizing an interception order to certify that:

- "[N]ormal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," 18 U.S.C. § 2518(3)(c), that
- The warrant contains "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates," *id*. § 2518(4)(c), that
- That the authorization is not allowed to last "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days" (though it can be renewed), *id*. § 2518(5), and that
- The interception "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under [Title III]." *Id*.

These rules have provided a strong basis for courts to ensure that searches do not go beyond the boundaries of "particularity" required by the Fourth Amendment. *See*, *e.g.*, *Torres*, 751 F.3d at 883–84 (applying the *Berger*-derived requirements to video surveillance).

A. The Ninth Circuit Established Workable Data Minimization Principles for Digital Search Cases

The Ninth Circuit's *per curiam* opinion in *Comprehensive Drug Testing* addressed the specific problem of applying the traditional plain view doctrine to digital files seized pursuant to a search warrant. *Comprehensive Drug Testing*, 621 F.3d at 1176–77. Judge Kozinski, in a concurring opinion joined by five other circuit judges, summarized the implications of the court's decision in order to

provide "guidance about how to deal with searches of electronically stored data in the future." *Id*. at 1179 (Kozinski, J., concurring). In particular, Judge Kozinski found that the following rules should guide law enforcement searches of digital files:

1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
2. Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1180 (Kozinski, J., concurring).

These principles create a workable solution for the problem of searching and seizing irrelevant information contained within electronic storage. The second and fourth principles are especially relevant to the case before the Court, as they recognize the importance of minimizing the intrusion on privacy by minimizing the search of irrelevant data.

The court in *Comprehensive Drug Testing* updated the principles first

established in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), which addressed the circumstances where segregation of non-pertinent files could not be completed onsite, to "apply to the daunting realities of electronic searches . . . ." *Comprehensive Drug Testing,* 621 F.3d at 1177. The *Tamura* rules are "well suited to the practical considerations involved in searching through computer memory." Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech 75, 107 (1994). According to the Ninth Circuit, "everyone's interests are best served if there are clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment." *Id*.

These guidelines serve as a useful framework for minimizing the search of data in cases involving electronic devices and information. Other courts have also recognized the value of data minimization principles to a person's privacy. *See, e.g. United States v. Wei Seng Phua,* No. 14-00249, 2015 WL 1281603 (D. Nev. Mar. 20, 2015) (requiring warrant execution rules consistent with the principles outlined in *Comprehensive Drug Testing*); *In re Search of Google Email Accounts Identified in Attachment A*, ___ F. Supp. 3d ___, 2015 WL 926619 (D. Ala. Mar. 3, 2015) (requiring that the government comply with principles four and five); *In re U.S.'s Application for a Search Warrant to Seize & Search Elec. Devices from Edward Cunnius*, 770 F. Supp. 2d 1138 (W.D. Wash. 2011) (finding that a search

warrant was overbroad where it did not comply with the principles outlined in *CDT*).

In addition, other courts have followed the Ninth Circuit's guidelines and required specific protocols for data minimization relating to electronic searches. *See*, *e.g.*, *In re Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 5–6 (D.D.C. 2013) (prohibiting the government from obtaining Facebook data about non-targets); *In re Black iPhone 4*, 27 F. Supp. 3d 74, 80 (D.D.C. 2014) (applying the rule that "'[s]egregation and redaction of electronic data must be done either by specialized personnel or an independent third party'"); *In re Search of Info. Associated with [redacted]@mac.com That is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1, 7 (D.D.C. 2014) (recommending the use of an independent search team, waiver of the plain view doctrine, a clear search protocol, and limitations on access to the data); *United States v. Cioffi*, 668 F. Supp. 2d 385 (E.D.N.Y. 2009) (noting that electronic data should be minimized by specifying a search protocol at the outset and using key term searches to identify relevant files); *United States v. Kim* 677 F. Supp. 2d 930, 347 (S.D. Tex. 2009) (granting motion to suppress based on failure to follow *CDT* guidelines).

The Second Circuit has also emphasized the need to critically examine use of the plain view doctrine in the digital context. *See United States v. Galpin*, 720

F.3d 436 (2d Cir. 2013) (suggesting that the court could be ready to consider applying guidelines similar to the ones adopted in *CDT*).

B. Courts Recognized the Importance of Data Minimization Principles Relating to Electronic Data Even Before Comprehensive Drug Testing

Even before the Ninth Circuit outlined the guidelines for digital searches in *Comprehensive Drug Testing*, federal courts recognized the importance of limiting searches that include large volumes of non-pertinent data. In *Andresen v. Maryland*, 427 U.S. 463 (1976), the Supreme Court recognized the importance of privacy in conducting searches of electronic records. The Court likened a search of telephone records to a search of a person's private papers, stating that, "In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Id*. at 482.

The Fifth Circuit and the United States Secret Service in *Steve Jackson Games v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), emphasized the value of keyword searches as a data minimization technique. The court found that the risk of searching irrelevant documents is lessened in the context of electronic communications, because "technology exists by which relevant communications can be located without the necessity of reviewing the entire contents of all of the stored communications . . . . For example, the Secret Service

claimed . . . that it reviewed the private email on the [electronic bulletin board system] by use of key word searches." *Id.* at 463. *See also* Winick, *supra* ("Whenever possible, key word searches should be used to distinguish files that fall within the scope of a warrant from files that fall outside the scope of a warrant.").

The Tenth Circuit in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), recognized that computers often contain "intermingled documents," and set forth several principles for the government to follow when handling massive quantities of electronic data. *See also United States v. Tamura,* 694 F.2d 591, 595–96 (9th Cir. 1982). Law enforcement officials in *Carey* exceeded the scope of their warrant to search the defendant's computers for evidence of possible sale and possession of cocaine by opening files containing child pornography. *Carey*, 172 F.3d at 1270–71. According to the court, "law enforcement must engage in the intermediate step of sorting various types of documents and then search the ones specified in the warrant." *Id.* at 1275. In accordance with this approach, the Tenth Circuit proffered several methods of data minimization to ensure that only relevant electronic documents are searched: "observing file types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory." *Id.* at 1276.

Similarly, the court in *United States v. Stierhoff*, 477 F. Supp. 2d 423 (D.R.I.

2007), found that defendants maintain a "legitimate expectation of privacy" in contents of non-relevant electronic files that are unrelated to the original purpose of a government search. The court found that "[w]here officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents." *Carey,* 172 F.3d at 1275. The court emphasized that "individuals undoubtedly have a high expectation of privacy in the files stored on their personal computers," *United States v. Adjani,* 452 F.3d 1140, 1146 (9th Cir. 2006), and found that consent to search one folder did not eliminate the defendant's expectation of privacy as to the contents of other files and folders on his computer. *Stierhoff,* 477 F. Supp. 2d at 443.

These legal principles were then incorporated into the *Comprehensive Drug Testing* guidelines, which address the privacy impacts of electronic searches. Giving the increasing importance of digital searches in most law enforcement investigations, it is essential that this Court adopt similar guidelines to limit the collection and storage of non-pertinent data. Courts have long recognized that "Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain

disclosure in court of what is whispered in the closet." *Olmstead v. United States*, 277 U.S. 438, 472-73 (1928) (Brandeis, J., dissenting). As a result of these technological developments, it is sometimes necessary to establish new constitutional safeguards.

CONCLUSION

Amici curiae EPIC et al. respectfully request that this Court rule in favor of the Appellants and affirm the panel decision.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
Counsel of Record
Alan Butler
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140
amicus@epic.org

July 29, 2015

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B). This brief contains 5,610 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word Mac in 14 point Times New Roman style.

Dated: July 29, 2015

/S/ MARC ROTENBERG

CERTIFICATE OF SERVICE

I hereby certify that on this 29th day of July, 2015, the foregoing Brief of *Amicus Curiae* was electronically filed with the Clerk of the Court, and thereby served upon counsel for the parties *via* electronic mail.

Dated: July 29, 2015

/S/ MARC ROTENBERG