No. 08-1332

IN THE

Supreme Court of the United States

CITY OF ONTARIO, CALIFORNIA, et al.,

Petitioners,

v.

JEFF QUON, et al.,

Respondents.

On a Writ of Certiorari to
The United States Court of Appeals
for the Ninth Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF THE RESPONDENTS

MARC ROTENBERG
Counsel of Record
JARED KAPROVE
GINGER MCCALL
KIMBERLY NGUYEN
JOHN VERDI
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

March 23, 2010

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.

EPIC has participated as *amicus curiae* in several cases before this Court and other courts concerning privacy issues, new technologies, and Constitutional interests, including *Doe v. Reed*, 529 F.3d 892 (9th Cir. 2008), *cert. granted*, 130 S. Ct. 1011 (U.S. Dec. 14, 2009) (No. 09-559); *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009); *Herring v. United States*, 129 S. Ct. 695 (2009); *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *National Cable*

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. *Amici* lodged with the Court Petitioners' and Respondents' letters of consent contemporaneous with the filing of this brief. In accordance with Rule 37.6, 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.

and Telecommunications Association v. Federal Communications Commission, 555 F.3d 996 (D.C. Cir. 2009); *Bunnell v. Motion Picture Association of America*, No. 07-56640 (9th Cir. filed Nov. 12, 2007); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006) 470 F.3d 1104 (5th Cir. 2006); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

EPIC has a longstanding interest in workplace privacy[2] and electronic message privacy[3] and has worked on several public awareness campaigns regarding these topics. In 2009, EPIC submitted a brief[4] in *Bunnell v. MPAA*.[5] EPIC's *amicus* brief supported the application of the federal Wiretap Act's protections to email messages in circumstances when the messages are briefly stored while they pass through mail servers. In *Bunnell*, a former employee hacked his ex-employer's corporate email server to secretly swipe private emails as they were transmitted. EPIC argued that the Wiretap Act applies to these sorts of circumstances by barring "interception" of electronic communications. EPIC has long advocated for application of the

---

[2] *See* EPIC: *Workplace Privacy*, http://epic.org/privacy/workplace/.

[3] *See* EPIC: *Gmail Privacy*, http://epic.org/privacy/gmail/faq.html.

[4] *See* EPIC: *Bunnel v. MPAA*, http://epic.org/privacy/bunnell/.

[5] *Bunnell v. Motion Picture Association of America*, No. 07-56640 (9th Cir. filed Nov. 12, 2007).

"interception" standard to email, and filed a 2004 *amicus* brief on this issue in *U.S. v. Councilman*.[6]

EPIC supports the right of public employees[7] to retain their privacy while engaging in personal communications while on the job. The Ninth Circuit's determination in the present case recognizes individuals' reasonable expectations of workplace privacy. Also, the Ninth Circuit established workable data minimization principles—principles that respect employees' expectations—in *Comprehensive Drug Testing*. If the Court overturns the Ninth Circuit in this case, it will dash millions of public employees' privacy expectations and subject personal communications to invasive government monitoring.

Technical Experts and Legal Scholars

Grayson Barber, Esq.
Grayson Barber, LLC

David Chaum
Chaum, LLC

---

[6] *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004).

[7] In *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987), the Court held that "[s]earches and seizures by government employers or supervisors of the private property of their employees, therefore, are subject to the restraints of the Fourth Amendment." Similar searches by private employers are not typically subject to Fourth Amendment restraints.

Julie E. Cohen
Professor of Law, Georgetown University Law Center

Simon Davies
Director General, Privacy International

David Farber
Professor of Computer Science and Public Policy, Carnegie Mellon University

Mary Minow
Library Law Consultant

Pablo G. Molina
Associate VP of IT and Campus CIO, Georgetown University

Peter G. Neumann
Principal Scientist, SRI International Computer Science Lab

Barbara Simons
IBM Research (Retired)

Latanya Sweeney
Distinguished Career Professor of Computer Science, Carnegie Mellon University

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

Government agencies may undertake reasonable searches of public employees, but they may not pursue unbounded searches of personal communications devices. Such activity is contrary to best practices in the security industry and would expose public employees to unnecessary risk. Modern communications devices reveal an extraordinary amount of personal data. The *Comprehensive Drug Testing* analysis describes a useful framework for safeguarding the privacy interests of public employees while providing government agencies the opportunity to undertake appropriate investigations.

ARGUMENT

I. Device Auditing Procedures that Do Not Respect Data Minimization Put Individuals At Risk

The principle of data minimization requires that auditors only collect and process personal information to the extent necessary to complete the audit. Strict adherence to this principle by public employers conducting investigatory searches is necessary to adequately protect the privacy and security of public employees.

A. Data Minimization is a Well-Established Principle of Information Technology Security

In 1973, the Department of Health, Education, and Welfare ("HEW") issued a report entitled "Records, Computers, and the Rights of Citizens." This report recommended that Congress enact legislation adopting a Code of Fair Information Practices for automated personal data systems.[8] The HEW report provides the basis for the principles of Fair Information Practices—principles that are now universally recognized.[9] The concept of data

---

[8] U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii (1973).

[9] *See* Federal Trade Commission, *Fair Information Practice Principles*, http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

minimization is inherent in Fair Information Practices. Data minimization requires that governments and other entities that collect and access individuals' personal information do so in a way that limits access and storage to the minimum amount of data necessary to accomplish a given task. Professor Spiros Simitis, while serving as the Data Protection Commissioner of the German state of Hesse, described this principle over 20 years ago:

> Personal information should only be processed for unequivocally specified purposes. Both government and private institutions should abstain from collecting and retrieving data merely for possible future uses for still unknown purposes. Both national and international organizations have in fact rejected the unlimited build-up of data files. In order to be retrieved, data must be necessary to a precise goal that is within the legally acknowledged activities of the organization interested in the information. A normative barrier thus prevents the technically possible multifunctional use of the data.[10]

Security experts agree that the best way to prevent loss or misuse of sensitive personal information is to avoid gathering or storing it in the

---

[10] Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 740 (1987).

first place.[11] In a proposed legal framework for government data mining, Fred H. Cate, professor of law and director of the Center for Applied Cybersecurity Research at the University of Indiana, suggests "[t]he use of data minimization and anonymization and other tools to limit the amount of information revealed to only what is necessary and authorized."[12] He goes further and identifies a number of tools and techniques so that "analysts can perform their jobs . . . without the need to gain access to personal data until they make the requisite showing for disclosure."[13]

One of the competitive advantages of leading firms and products in the electronic discovery sector is measured by how well they implement data minimization, that is, by how well they can search a corpus of information and return only those data elements that are relevant to the discovery.[14] Judging

---

[11] Larry Dignan, *When it Comes to Data, Less is Better*, eWeek (May 3, 2005), http://www.eweek.com/c/a/Data-Storage/When-it-Comes-to-Data-Less-is-Better/.

[12] Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 488 (2008).

[13] *Id.* at 488–89.

[14] *E.g.*, Hemanth Salem & James Ramsey, *Advanced Practices in Data Minimization*, Encore Discovery Solutions, http://www.encorelegal.com/discoveries/data_minimization.html; Inventus, *Case Study: In-House Data Minimization*, http://www.inventus.com/wp-content/uploads/2010/02/Inventus_Case-Studies_In-

by the wide availability of commercial technology products and services for data classification, protection and leak prevention, the state of technology is such that employers can investigate easily some elements of employee communications without gaining access to the content of the communications.

If sensitive information must be stored and accessed, the principle of data minimization requires that the smallest possible amount of information be used. Congress has acknowledged the importance of data minimization. For example, the amendments to the Foreign Intelligence Surveillance Act require adoption of minimization procedures as appropriate for all data acquisitions authorized under the section.[15] The definition of "minimization procedures" is set forth in two different portions of the statute, one for physical searches[16] and one for electronic surveillance.[17]

The two definitions include four types of procedures: procedures "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons;" procedures to prevent the unnecessary dissemination of

---

House-Data-Minimization1.pdf; Modus, *Electronic Discovery*, http://www.discovermodus.com/edisc.pdf.

[15] 50 U.S.C. § 1881a(e)(1) (2009).

[16] 50 U.S.C. § 1821(4) (2009).

[17] 50 U.S.C. § 1801(h) (2009).

nonpublicly available information "in a manner that identifies any United States person, without such person's consent;" procedures that require the disposal within 72 hours of the "contents of any communication to which a United States person is a party" acquired without a court order unless a new court order is obtained allowing retention, disclosure, or dissemination; and procedures that allow for exceptions to the retention and dissemination restrictions with respect to criminal evidence.[18] These terms demonstrate Congress's awareness that acquisition limitations are necessary but not sufficient, and that limitations on the government use of sensitive personal information are also required. These terms are mirrored in other statutes governing similar searches, including the provisions for investigatory wiretaps in the criminal context.[19]

B. In the Absence of Data Minimization, Public Employees Would Be Exposed to Unnecessary Risk

Data minimization is classified as a security method as much a privacy protection.[20] In fact, while speaking on a recent panel on Information Security Best Practices, two professors at the Wharton School of Business characterized the retention of personal

---

[18] 50 U.S.C. § 1801(h) (2009).

[19] 18 U.S.C. § 2518(5) (2009).

[20] Dignan, *supra* note 11 (noting that minimization practices "won't end the theft of customer information, but it will limit what data there is to steal (or lose)").

data as "increasingly a liability for companies" concerned about the risks of data breaches.[21]

In 2008, a group of six security experts analyzed the Protect America Act of 2007,[22] the amendments to the Foreign Intelligence Surveillance Act, looking for potential security hazards of the statutory scheme. These researchers included Whitfield Diffie of Sun Microsystems and Peter G. Neumann, a well-known expert in information security. They concluded that "minimization matters," specifically finding that "[a]n architecture that minimizes collection of communications lowers the risk of exploitation by outsiders and exposure to insider attacks. . . . It should be fundamental to the system's design that the combination of interception location and selection methods minimizes the collection of purely domestic traffic."[23]

In *O'Connor v. Ortega*, this Court held that "public employer intrusions on the constitutionally protected privacy interests of government employees for . . . investigations of work-related misconduct should be judged by the standard of reasonableness."[24] Under the reasonableness

---

[21] Forbes, *What Personal Data Should You Keep—And Toss?* (Mar. 19, 2009), *available at* http://www.forbes.com/2009/03/19/heartland-payment-security-entrepreneurs-sales-marketing-security.html.

[22] Pub. L. No. 110-55, 121 Stat. 552 (2007).

[23] Steven M. Bellovin, et al., *Risking Communications Security: Potential Hazards of the Protect America Act*, IEEE SECURITY & PRIVACY, Jan.–Feb. 2008, at 24, 31.

[24] *O'Connor v. Ortega*, 480 U.S. 709, 725 (1987).

standard, "one must determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place.'"[25] Given the widespread acceptance of data minimization as a principle of electronic security, an electronic search that fails to employ data minimization techniques is unreasonable.

II. Communications Devices Reveal Sensitive Personal Information

Employer-issued communications devices access sensitive personal information in a variety of ways. They are capable of accessing the internet, sending and receiving electronic messages, and collecting locational data.

A. Many Employers Issue and Monitor Sophisticated Communications Devices to Employees

Many employers pay for cellphones, smartphones, and laptops that are issued to employees. A recent *USA Today* poll found that 59% of professionals reported that their employer paid for the laptop they regularly use for work.[26] Fifty-six percent of professionals said that their employer paid for their smart phone.[27] Twenty-four percent said

---

[25] *Id.* at 726 (quoting *Terry v. Ohio*, 392 U.S. 1, 20 (1968)).

[26] Michelle Kessler, *Some Employees Buy Own Laptops, Phones for Work*, USA Today, June 16, 2008, *available at* http://www.usatoday.com/money/workplace/2008-06-15-electronic-devices-workplace_N.htm.

[27] *Id.*

that their employer paid for their regular cellphone.[28] And 21% of employees surveyed said that their employer paid for their Personal Digital Assistant.[29] The article also reported that since most employees are not going to use or carry two cellphones or laptops, company-issued equipment usually gets used for non-work purposes.[30]

The smartphones that employers often buy for employees boast a variety of features. Apple, the maker of the iPhone, boasts that

> iPhone uses fast 3G and Wi-Fi wireless connections to deliver rich HTML email, Maps with GPS, and Safari—the most advanced web browser on a mobile device. It has Google and Yahoo! search built in. And since iPhone multitasks, you can make a phone call while emailing a photo or surfing the web over a Wi-Fi or 3G connection.[31]

The iPhone includes features that allow users to make phone calls, send text messages, send emails, surf the internet, and play media files. Blackberry smartphones, products of Research in Motion, boast similar features. Blackberry devices allow users to send and receive email, send and receive text

---

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Apple, *iPhone: Find Out Why You'll Love iPhone*, http://www.apple.com/iphone/why-iphone/.

messages and phone calls, instant message with friends and colleagues, browse the internet, use GPS applications, and play media files (among other things).[32] Palm and several other companies manufacture similar devices. These smartphones rely on a "3G" Network, which allows simultaneous use of speech and data services and higher data rates than older networks.

Ordinary cell phones also offer many of these features. Companies such as Motorola, Samsung, and LG offer cell phones that can access the internet, send and receive emails, make phone calls, and send and receive text messages.

At the same time that many employers are issuing mobile communication devices to employees, the employers are also monitoring those devices. A 2007 Electronic Monitoring Surveillance Survey by the American Management Association, polled employers, including public employers, about their companies' monitoring practices. More than half of employer respondents reported that their organization monitors all employees' internet usage.[33] An additional 14% indicated that the organization monitors the internet usage of selected categories of employees.[34] Twenty-eight percent of

---

[32] Blackberry, *Blackberry Smartphones*, http://na.blackberry.com/eng/devices/.

[33] American Management Association, *Electronic Monitoring Surveillance Survey*, Feb. 2008, *available at* http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/.

[34] *Id.*

responding employers reported that they monitor all employees' computer use for time spent, matter/content, or keystrokes entered.[35] Another 17% reported that they monitor the computer use of selected job categories.[36] Twenty-five percent of employers reported that they store and review all employees' computer files.[37] Another 18% reported that they store and review some employees' computer files.[38]

Forty-three percent of employers reported that they monitored at least some employees' email.[39] Of those employers, 96% monitored external email (incoming and outgoing), and 58% monitored internal email (sent among employees).[40] One in ten of those employers reported that their employees do not know about the organization's policy of monitoring email.[41]

Forty-five percent of employers indicated that their organization monitors at least some employees' telephone usage (time spent and numbers called).[42] Sixteen percent of those employers report that their employees do not know about the organization's policy of monitoring telephone use.[43]

---

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

B. Employer-Issued Communications Devices Reveal Internet Browsing History and Web Search Data

Mobile devices, including those issued by employers, have also become an increasingly popular way to access the internet. A 2009 Pew Research Center study reported that 55% of American adults connect to the internet wirelessly, either through a WiFi or WiMax connection via their laptops or through their handheld device like a smart phone.[44] The same study reports that more than half of 18- to 29-year-olds have accessed the internet wirelessly on a cell phone (55%). A global study conducted by market research firm Synovate found that 17% of respondents use internet browsing on their mobile phones, including 31% of U.K. respondents and 26% of U.S. respondents.[45]

These mobile devices can easily access web search and record web search history. Search engines are engaged in intense competition to provide default

---

[44] Pew Research Center, *Internet, Broadband, and Cell Phone Statistics*, Jan. 5, 2010, *available at* http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.

[45] Synovate, *Global Survey Shows that Cell Phone is 'Remote Control' for Life*, Sept. 17, 2009, http://www.synovate.com/news/article/2009/09/global-survey-shows-cell-phone-is-remote-control-for-life-42-of-americans-can-t-live-without-it-and-almost-half-sleep-with-it-nearby.html.

search service on cell phones and smart phones.[46] Google and Bing competed with each other and a variety of other search engine companies to become the default searches for iPhones and Verizon mobile devices (respectively). [47] Companies such as Microsoft and Google have designed specialized search engines for cell phone and smart phone users.[48] Google advertises that its new version of Custom Search "enables a rich interactive mobile experience on high-end devices such as Android-powered phones, iPhone, iPod touch, and Palm Pre."[49]

C. Employer-Issued Communications Devices Reveal Messaging Data

Laptops, cell phones, and smart phones are all able to send messages to outside recipients. All three can employ email technology and all three are

---

[46] Cade Metz, *Verizon Snuffs Google for Microsoft Search*, Register, Dec. 19, 2009, http://www.theregister.co.uk/2009/12/19/verizon_snuffs_google_for_bing.

[47] *Id.*; William Hobson, *How Smartphone Users Use E-commerce Sites Via Mobile*, Vertical Leap, Feb. 18, 2010, http://www.vertical-leap.co.uk/news/how-smartphone-users-use-ecommerce-sites-via-mobile/.

[48] Sharon Pian Chan, *Microsoft Unveils New Smartphone Software*, Seattle Times, Feb. 16, 2010, http://seattletimes.nwsource.com/html/microsoftpri0/2011096322_microsoftunveilsnewsmartphonesoftware.html.

[49] Google, *Google Custom Search for Your Smartphone,* Oct. 22, 2009, http://googlecustomsearch.blogspot.com/2009/10/google-custom-search-for-your.html.

capable of sending text messages; laptops can use email accounts to send text messages to mobile devices.

Many users take advantage of this technology and use mobile devices to send text messages. A 2009 study conducted by Consumers Union found that nearly 70% of respondents used their cell phones to send or receive text messages.[50] According to a Nielsen Mobile survey released 2008, for the second quarter of 2008, U.S. mobile subscribers sent and received on average 357 text messages per month.[51] Another study by CTIA Wireless Association found that over 740 billion text messages were sent over carrier networks in the U.S. during the first half of 2009.[52] That is 4.1 billion text messages being sent daily (nearly twice as many as were sent during the same period the previous year).

---

[50] Consumer Union, *Consumer Reports Survey Found Cell-Phone Service Providers Among Lower-Rated Services*, Dec. 1, 2009, http://www.prnewswire.com/news-releases/consumer-reports-survey-found-cell-phone-service-providers-among-lower-rated-services-78272857.html.

[51] Neilson Wire, *In U.S., SMS Text Messaging Tops Mobile Phone Calling*, Sept. 22, 2008, http://blog.nielsen.com/nielsenwire/online_mobile/in-us-text-messaging-tops-mobile-phone-calling/.

[52] CTIA Wireless Association, *The Wireless Association Announces Semi-Annual Wireless Industry Survey Results*, Oct. 7, 2009, http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20091007006200&newsLang=en.

In a global study 17% of respondents reported using email on their mobile on a regular basis, including 26% in the US and 25% in the UK.[53] These findings were corroborated in another recent survey, where more than 20% of survey respondents reported using their cell phone to check email at least occasionally.[54]

D. Employer-Issued Communications Devices Reveal Locational Data

Many smartphones are equipped with Global Positioning ("GPS") capabilities. GPS is a satellite-based service that enables individuals to determine their precise location anywhere on Earth. The U.S. government operates GPS, and provides free access to the public.[55] Anyone can use an electronic device containing a GPS receiver to access GPS signals and determine their precise location, altitude, and speed.[56] Many smartphones, including Apple's iPhone, several Blackberry models, and Palm's Treo, have a built-in GPS receiver, which allows users to

---

[53] Synovate, *supra* note 45.

[54] PC Pitstop, *Cell Phone & PC Usage Survey*, Jan. 2009, http://techtalk.pcpitstop.com/2009/01/26/cell-phone-pc-usage-survey-results/.

[55] 10 U.S.C. § 2281(b) (2009) (requiring the U.S. Dep't. of Def. to provide GPS "for peaceful civil, commercial, and scientific uses on a continuous worldwide basis free of direct user fees").

[56] U.S. Air Force, *Global Positioning System Fact Sheet*, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5325.

make use of GPS mapping and location-based check-in.[57]

Even employer-issued devices that do not have GPS capabilities can collect and maintain reasonably specific locational data. A phone, even when it is not engaged in an active call, can emit a roaming signal. This signal gets picked up by the next nearby cell phone antenna tower.[58] This reveals the cell phone's location. More detailed locational information can be obtained by interpolating signals between adjacent antenna towers.[59] Some services achieve a precision of down to 50 meters in urban areas where mobile traffic and density of antenna towers (base stations) is sufficiently high.[60] Rural and desolate areas may see miles between base stations and therefore determine locations less precisely.[61] This locational data is then held by phone companies. The data can be disclosed to law enforcement for legitimate purposes, including emergency services, but also poses a significant risk to privacy of phone users if it is disclosed without proper legal process.

Employer-issued mobile devices without GPS can also track individuals by using wireless internet connections. When a phone or other mobile device is in range of a wireless router, the router, which has a

---

[57] *E.g.*, Blackberry, *GPS Capabilities*, *http://na.blackberry.com/eng/devices/features/gps.jsp.*

[58] *Mobile Phone Tracking*, Wikipedia, http://en.wikipedia.org/wiki/Mobile_phone_tracking.

[59] *Id.*

[60] *Id.*

[61] *Id.*

known geographic location, is then used to associate the phone with the geographic location.[62] This allows devices to be uniquely identified and associated with a particular location.

Hybrid methods are also used to track mobile devices. These methods use a combination of GPS, cell tower information, and wireless positioning. [63]

E. Users' Internet Browsing Histories, Search Data, Electronic Messages, and Locational Data are Sensitive Personal Information

Courts and legislatures recognize the sensitivity of information concerning individuals' internet browsing, web searches, electronic messages, and location. For example, federal laws prohibit private parties from intercepting Internet communications, bar companies from disclosing records of past Internet activity, and limit government access to users' data.[64] Federal courts recognize individuals' interests in keeping "their use of the Internet or other communications media" free from surveillance.[65]

---

[62] Skyhook Wireless, *How it Works*, http://www.skyhookwireless.com/howitworks/.

[63] *Id.*

[64] *See, e.g.*, 18 U.S.C. § 2511 (2009) (prohibiting interception); 18 U.S.C. § 2702 (2009) (barring disclosure of stored communications); 18 U.S.C. § 3121(c) (2009) (limiting government access).

[65] *Gonzalez v. Google*, 234 F.R.D. 674, 678 (N.D. Cal. 2006).

To protect this privacy interest, courts often require litigants to de-identify or mask information that would identify users' internet browsing histories from documents disclosed during litigation.[66] Users' interests in freedom from surveillance are particularly acute when Internet search queries are disclosed. "Search queries themselves may constitute potentially sensitive information," implicating "privacy issues raised by [a government] request for the text of search queries."[67]

Federal law prohibits interception of Internet browsing activity, search data, and electronic messages.[68] The Wiretap Act provides for civil liability and criminal penalties against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any . . . electronic communication [except as provided in the statute]."[69] The Act imposes

---

[66] *E.g.*, *Columbia Pictures v. Bunnell*, No. 06-1093, 2007 U.S. Dist. LEXIS 46364 at *47 (C.D. Cal. May 29, 2007); *Columbia Pictures v. Fung*, No. 06-5578, 2007 U.S. Dist. LEXIS 97576 (C.D. Cal. June 8, 2007); *see also Keith H. v. Long Beach Unified School District*, 228 F.R.D. 652, 657 (C.D. Cal. 2005) (noting "federal courts ordinarily recognize a constitutionally-based right of privacy that can be raised in response to discovery requests.").

[67] *Gonzalez*, 234 F.R.D. at 687.

[68] 18 U.S.C. § 2511 (2009).

[69] 18 U.S.C. § 2511(1)(a) (2009); *see also United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994) (defining

identical liability on any person who intentionally discloses the contents of an intercepted communication.[70] The Act also states:

> a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.[71]

Internet traffic, including browsing history, search data, and email and chat communications constitute "electronic communications."[72]

Federal law also prohibits disclosure of records detailing users' past Internet activities.[73] The Stored Communications Act prohibits service providers from

---

"interception" as "acquisitions contemporaneous with transmission.").

[70] 18 U.S.C. § 2511(1)(c)-(d) (2009).

[71] 18 U.S.C. § 2511(3)(a) (2009).

[72] *In re Doubleclick Privacy Litigation*, 154 F. Supp. 2d 497, 508 n.18 (S.D.N.Y. 2001) (citing 18 U.S.C. § 2510(15) (2009) and 18 U.S.C. § 2510(12) (2009)).

[73] 18 U.S.C. § 2702 (2009).

"knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service."[74] The Act provides for civil liability and criminal penalties for unlawful disclosure.[75] Courts have strictly construed the Act and prohibited disclosure of users' stored communications in a variety of circumstances, including in cases involving otherwise proper civil discovery subpoenas.[76]

Similarly, locational data receives special protection. Courts require law enforcement officers to obtain a warrant before tracking drivers—even when they travel openly on public roads.[77] Locational information is particularly sensitive because it can reveal:

> . . . a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise

---

[74] 18 U.S.C. § 2702(a)(1) (2009).

[75] 18 U.S.C. § 2701 (2009); 18 U.S.C. § 2707 (2009).

[76] *See, e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 609 (E.D. Va. 2008); *FTC v. Netscape*, 196 F.R.D. 559, 559, 561 (N.D. Cal. 2000).

[77] *Commonwealth v. Connolly*, 454 Mass. 808, 810 (Mass. 2009); *People v. Weaver*, 12 N.Y.3d 433, 445 (N.Y. 2009); *State v. Jackson*, 76 P. 3d 217, 223 (Wash. 2003); *State v. Campbell*, 759 P.2d 1040, 1048 (Or. 1988). *But see United States v. McIver*, 186 F.3d 1119, 1127 (9th Cir. 1999); *United States v. Jones*, 451 F. Supp. 2d 71, 88 (D.D.C. 2006).

> gyms, places where children are dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the 'wrong' side of town, the family planning clinic, and the labor rally.[78]

The Supreme Court of Washington observes that locational data receives greater legal protection than other types of information because it "can reveal preferences, alignments, associations, personal ails and foibles."[79] It can "provide a detailed picture of one's life."[80]

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

In *Comprehensive Drug Testing v. United States*,[81] the Ninth Circuit established specific data minimization requirements for electronic data searches by law enforcement officers. This framework sets out a strong set of principles for digital searches that allows the government to pursue appropriate investigations while ensuring that access to electronic data does not become unbounded. The facts of the text messaging case now before the Supreme Court show how the government's interest in recovering the payment for the text messaging services can be satisfied without allowing the search of the content of the messages.

---

[78] *State v. Jackson*, 76 P. 3d at 262.

[79] *Id.*

[80] *Id.*

[81] 579 F.3d 989 (9th Cir. 2009).

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

1. Comprehensive Drug Testing: The Framework

Comprehensive Drug Testing v. United States outlines five principles relating to government examination and seizure of electronic 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.[82]

These principles create a workable solution for the problem of searching and seizing irrelevant information contained in electronic data. 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.

Citing *United States v. Tamura*,[83] in which the court delineated procedural guidelines for seizing "intermingled documents" at the scene of a search, *Comprehensive Drug Testing* updates the *Tamura* principles to "apply to the daunting realities of electronic searches . . . ."[84] One legal scholar wrote that the *Tamura* rules are "well suited to the practical considerations involved in searching through computer memory."[85] 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

---

[82] *Comprehensive Drug Testing*, 579 F.3d at 1006.

[83] 694 F.3d 591 (9th Cir. 1982).

[84] *Comprehensive Drug Testing*, 579 F.3d at 1006.

[85] Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH 75, 107 (1994).

the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment."[86]

Comprehensive Drug Testing involved an electronic search of records resulting from a federal investigation into the use of performance-enhancing drugs by professional baseball players. After federal authorities learned that ten baseball players had tested positive for steroids in their urine samples administered by Comprehensive Drug Testing, Inc. ("CDT"), the government obtained a warrant authorizing the search of CDT records pertaining to those ten players.[87] However, when the search was executed, the government seized and reviewed drug testing records for hundreds of players in Major League Baseball.[88] Evaluating the three judicial orders involved, the Ninth Circuit found that "this was an obvious case of deliberate overreaching by the government in an effort to seize data . . . ."[89]

The court went on to explain that the government failed to adhere to procedures outlined in *United States v. Tamura*.[90] Because searches of electronic records are becoming increasingly prevalent, the Ninth Circuit proffered five data minimization techniques to follow when the government wishes to "examine a computer hard drive or electronic storage medium in searching for

---

[86] *Id; see also* U.S. CONST. amend. IV.

[87] *Comprehensive Drug Testing*, 579 F.3d at 993.

[88] *Id.*

[89] *Id.* at 1000.

[90] *See Tamura*, 694 F.3d 591.

certain incriminating files . . . ."[91] The guidelines include having an independent third party segregate and redact the electronic documents, and creating a search protocol that only uncovers relevant information for which the government has probable cause.[92]

While at least one of the prescriptions proffered by the Ninth Circuit has been met with criticism,[93] the guidelines, as a whole, serve as a useful framework for minimizing the search of data in cases involving electronic devices and information. *Comprehensive Drug Testing* highlights the importance of data minimization in electronic searches, and other courts, whether or not they

---

[91] *Comprehensive Drug Testing*, 693 F.3d at 1006.

[92] *Id.*

[93] *See, e.g.*, *Recent Case: Fourth Amendment - Plain View Doctrine - En Banc Ninth Circuit Holds that the Government Should Waive Reliance on Plain View Doctrine in Digital Contexts.* - United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc)*, 123 HARV. L. REV. 1003 (2010) ("In effect, [one of the] requirement[s] would eliminate the plain view doctrine in electronic discovery cases. Such broad prescriptions are both unnecessary to the court's decision and detrimental to what would otherwise be legitimate searches by law enforcement agents."); *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010) ("Although the Ninth Circuit's rules provide some guidance in a murky area, we are inclined to find more common ground with the dissent's position that jettisoning the plain view doctrine entirely in digital evidence cases is an 'efficient but overbroad approach.'" (internal citation omitted)).

followed the specific guidelines of the Ninth Circuit, have also recognized the value of data minimization principles to a person's privacy.

2. *Comprehensive Drug Testing*: Progeny

Since *Comprehensive Drug Testing* was decided just a few months ago, other courts have followed the Ninth Circuit's guidelines and required specific protocols for data minimization relating to electronic searches. A New York federal district court in *United States v. Cioffi*[94] recognized that "[t]he dawn of the Information Age has only heightened those concerns [about privacy.]"[95] In finding that a warrant the FBI relied upon in searching a defendant's personal email account was unconstitutionally broad, the court outlined ways that other courts and commentators "have wrestled with how best to balance privacy interests and legitimate law-enforcement concerns in the context of computer searches."[96] Turning to a law review article as guidance, the court noted that one way to minimize the search of electronic data is to specify a search protocol at the outset and to use key word searches to extract only relevant files.[97] Further, according to the court, the creation of firewalls would prevent investigators from obtaining computer files before a third party has segregated

---

[94] 2009 U.S. Dist. LEXIS 99409 (E.D.N.Y. Oct. 26, 2009).

[95] *Id.* at *14.

[96] *Id.*

[97] *See* Winick, *supra* note 85.

relevant from non-relevant files.[98] Quoting *Comprehensive Drug Testing*, "segregation and redaction must be either done by specialized personnel or an independent third party [and t]he 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."[99]

The court in *United States v. Kim*[100] followed the reasoning and guidelines in *Comprehensive Drug Testing* to suppress evidence of an electronic search that uncovered child pornography. In *Kim*, the Government executed a search warrant and searched defendant Kim's hard drives, laptop, and desk computers, for evidence of "computer intrusion," as described in 18 U.S.C. § 1030.[101] While searching Kim's electronic files, the Government came across JPEG files believed to be child pornography, and charged Kim with an additional count of possessing child pornography.[102] Kim moved to suppress the evidence, and the court did so, citing *Comprehensive Drug Testing* to say that the Government's actions were "an obvious case of deliberate overreaching by

---

[98] *Cioffi*, 2009 U.S. Dist. LEXIS 99409, at *15.

[99] *Id.* at *15-16 (*quoting Comprehensive Drug Testing v. United States*, 579 F.3d 989, 1006 (9th Cir. 2009)).

[100] 2009 U.S. Dist. LEXIS 121871 (S.D. Tex. Dec. 24, 2009).

[101] *Id.*

[102] *Id.*

the government in an effort to seize data . . . ."[103] The court reasoned that the Government's search was "clearly not conducted in accordance with the narrow guidelines promulgated in *Comprehensive Drug Testing*," and suggested the agent could have minimized the data searched by relying on the files' last created or modified date, which reflects the last date a file was manipulated, rather than last access date of the files.[104]

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

Electronic storage contains a "greater quantity and variety of information than any previous storage method," making computers and other electronic devices the subject of searches for incriminating information.[105] In *Andresen v. Maryland*,[106] the Supreme Court recognized the importance of privacy in searching such devices. 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

---

[103] *Id.* at *43 (*quoting Comprehensive Drug Testing*, 579 F.3d at 1000).

[104] *Id.* at *45-47.

[105] Winick, *supra* note 85.

[106] 427 U.S. 463 (1976).

manner that minimizes unwarranted intrusions upon privacy."[107]

The Fifth Circuit and the United States Secret Service in *Steve Jackson Games v. United States Secret Service*[108] 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 e-mail on the BBS by use of key word searches."[109]

The Tenth Circuit in *United States v. Carey*[110] recognized that computers often contain "intermingled documents," and set forth several principles for the Government to follow when handling massive quantities of electronic data.[111] 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

---

[107] *Id.* at 482.

[108] 36 F.3d 457 (5th Cir. 1994).

[109] *Id.* at 463. *See also* Winick, *supra* note 85 ("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.").

[110] 172 F.3d 1268 (10th Cir. 1999).

[111] *See also United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982).

child pornography.[112] 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."[113] 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."[114]

Similarly, the court in *United States v. Stierhoff*[115] 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. In *Stierhoff*, the defendant consented to a search of a specific folder on his computer for evidence of stalking, but was subsequently indicted for tax evasion once an IRS computer specialist discovered evidence of tax fraud in a folder outside the specified directory.[116] The court granted a motion to suppress the evidence of tax evasion, citing *Carey* to state that "[w]here offices 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

---

[112] *Carey*, 172 F.3d at 1270-71.

[113] *Id.* at 1275.

[114] *Id.* at 1276.

[115] 477 F. Supp. 2d 423 (D.R.I. 2007).

[116] *Id.* at 426-27.

further search through the documents."[117] Recognizing that "individuals undoubtedly have a high expectation of privacy in the files stored on their personal computers,"[118] the court found that although the defendant gave consent to search one folder on his computer, he maintained an expectation of privacy as to the contents of other files and folders on his computer.[119]

The principles set forth in *Comprehensive Drug Testing* provide guidance to the Government on how to minimize the search of irrelevant information in electronic data. These principles, which have been accepted by several other courts, balance the government's need to search against the privacy rights of citizens. This Court should consider the importance of search minimization in protecting against unwarranted intrusions on privacy.

---

[117] *Carey*, 172 F.3d at 1275.

[118] *U.S. v. Adjani*, 452 F.3d 1140, 1146 (9th Cir. 2006).

[119] *Stierhoff*, 477 F. Supp. 2d at 443.

CONCLUSION

Amici respectfully request this Court to grant Respondents' motion to affirm the decision of the lower court.

Respectfully submitted,

MARC ROTENBERG
JARED KAPROVE
GINGER MCCALL
KIMBERLY NGUYEN
JOHN VERDI
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
p: (202) 483-1140
f: (202) 483-1248
rotenberg@epic.org

March 23, 2010