October, 2014

'I Know My Rights, You Go'n Need a Warrant For That:' The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds

Laurie Buchan Serafino, *Duquesne University School of Law*

DUQUESNE UNIVERSITY
SCHOOL OF LAW

LEGAL STUDIES RESEARCH PAPER SERIES

"I Know My Rights, So You Go'n Need A Warrant For That": The Fourth Amendment, Riley's Impact, And Warrantless Searches of Third-Party Clouds

Laurie Buchan Serafino
Associate Professor of Law
Director of Clinical Legal Education

2013

Duquesne University School of Law Research Paper
No. 2013-08
Final Version (2/2015)

Originally published in BERKELEY JOURNAL OF CRIMINAL LAW (Fall 2014)

"I Know My Rights, So You Go'n Need A Warrant for That": The Fourth Amendment, *Riley*'s Impact, And Warrantless Searches of Third-Party Clouds

Laurie Buchan Serafino*

* Associate Professor of Law, Director, Tribone Center for Clinical Legal Education, Duquesne University School of Law. This article is dedicated to the memory of my mother, Esther Adelman (1924–2013), blessed be her memory. I would like to thank Harvard Law School Librarian Jennifer Allison for Foreign, Comparative, and International Law, Duquesne University Associate Dean for Faculty Scholarship and Professor Jane Campbell Moriarty, Duquesne University Associate Dean of Academics and Professor of Law Bruce Ledewitz, and Duquesne University Associate Professor and Director of Criminal Law Wesley Oliver. Many law students assisted in the preparation of this article. Special thanks to Pepperdine University School of Law research assistants Leor Makeover and Brittany Thomas and Duquesne University School of Law research assistant Mary O'Rourke. In particular, I would like to thank William and Mary Law School student Abigail J. Snider.

I. INTRODUCTION

"Them Feds Don't Play Fair"[1]

Technological advancements in the twenty-first century have complicated the task of determining what information we can reasonably expect to remain private under the Fourth Amendment as we store and access more information online.[2] What are the Fourth Amendment implications of electronically stored data? Among other things, should users who store material on cloud-based systems be entitled to protection from government inspection of that information even though they sign licensing agreements with third-party Internet Service Providers (ISPs)?

Without first obtaining a court order, the government is now accessing, obtaining and storing our online data.[3] Edward Snowden's disclosure of highly secretive National Security Administration (NSA) program information illustrated that the government has the means to thoroughly monitor our online activity.[4] Americans deserve greater

---

[1] JAY-Z, *99 Problems*, *on* THE BLACK ALBUM (Roc-A-Fella Records 2003).

[2] The Fourth Amendment to the United States Constitution recognizes a "right of the people to be secure in their persons, houses, papers, and effects" and protects its citizens from "unreasonable searches and seizures." U.S. CONST. amend. IV.

[3] Since 2006, the "NSA has collected the records of everyone, then returned to a secret federal court to get authorization to target specific individuals more closely." Philip Ewing, *NSA Memo Pushed to 'Rethink' 4th Amendment*, POLITICO, http://www.politico.com/story/2013/06/nsa-memo-4th-amendment-92416.html (last updated June 9, 2013, 6:49 PM). Although PRISM allows for broad, sweeping collection of data, a court order from the Foreign Intelligence Surveillance Court (FISC) is required to obtain specific data from tech companies. Dan Roberts et al., *Clapper Admits Secret NSA Surveillance Program to Access User Data*, THE GUARDIAN (June 7, 2013, 11:03 AM), http://www.guardian.co.uk/world/2013/jun/07/clapper-secret-nsa-surveillance-prism. The problem with this approach is that the government has access to private user data before it is required to obtain a court order. *Id.* The government claims that it cannot determine which individuals it intends to target without first sifting through large amounts of data, gathered during broad, sweeping searches. *Id.*

[4] *See* Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA*

Fourth Amendment protection and transparency from a government that is unchecked by outside regulators. Yet at the same time, concerns about terrorism and national security are uppermost in our minds, with a new atrocity committed nearly every day. We must determine once again where on the spectrum the proper Fourth Amendment balance lies between security and liberty.

Complicating the matter is the third-party doctrine, which evolved from the reasonable expectation of privacy test.[5] This doctrine provides that any information knowingly exposed to a third party loses Fourth Amendment protection because, by voluntarily sharing this information, one assumes the risk that the third party would divulge the information to the government.[6]

Federal statutes do little to remedy the confusion caused by the third-party doctrine. For instance, the Stored Communications Act (SCA), created to limit the government's ability to compel public ISPs to disclose information they store and to limit a provider's ability to voluntarily disclose information to both governmental and non-governmental entities,[7] may not apply to stored data and allows the

Surveillance Revelations, THE GUARDIAN (June 11, 2013, 9:00 AM), http://gu.com/p/3gec7/sbl. In early June 2013, Edward Snowden, an employee of Booz Allen Hamilton, contractor for the NSA, leaked highly sensitive information about a secret surveillance program, PRISM, which was established in 2008 through the Foreign Intelligence Surveillance Act (FISA) Amendments. *See* Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST (June 12, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date. The NSA's access to data through PRISM is "governed by Section 702 of the [FISA]." *Id.*

The NSA uses PRISM to monitor Internet and email traffic as it enters and leaves the United States, collecting private user data from nine major Internet companies. *Id.* PRISM is merely "a small part of a massive domestic dragnet run by the nation's premier covert intelligence gathering organization." Michael B. Kelley, *The Best Explanation Yet Of How the NSA's PRISM Surveillance Program Works*, BUS. INSIDER (June 15, 2013, 2:22 PM), http://www.businessinsider.com/how-prism-surveillance-works-2013-6.

James Clapper, Director of National Intelligence, has confirmed that the NSA uses major Internet companies "to obtain information that includes the content of emails and online files." Roberts et al., *supra* note 3.

[5] *See* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

[6] *See Miller*, 425 U.S. at 443; *Smith*, 442 U.S. at 743–44.

[7] *See* 18 U.S.C. § 2702 (2008) (prohibiting persons or entities that provide electronic communication services or remote computing services to the public from knowingly divulging contents of users' communications, except in limited circumstances).

government easy access to content-based information.[8]

The Foreign Intelligence Surveillance Act (FISA) provides less protection than the SCA. FISA was enacted in 1978 "to protect U.S. persons while allowing the government to monitor the activities of foreign powers and agents of foreign powers in the United States."[9] The government can obtain the content-based information of United States citizens without a showing of probable cause, which may render FISA unconstitutional as applied to United States citizens.[10] Under FISA, incidental third parties can be participants in intercepted communications with targets being investigated by the government.[11] FISA statutes are not limited to surveillance that is aimed at international terrorism.

This article consists of four parts. Part I traces the history of electronic privacy, examines the third-party doctrine, and discusses the application of the Fourth Amendment to cloud computing. It concludes that information voluntarily disclosed to automated third-party Internet Service Providers (ISPs) should not, for that reason alone, be deprived of Fourth Amendment protection. Part II suggests that there should be a presumption that cloud-based data is protected by the Fourth Amendment and recommends factors, based upon Supreme Court jurisprudence, which could rebut that presumption. These factors include: whether an individual made efforts to keep her information private, whether the information is content-based, whether the information reveals intimate details of an individual's life, whether shared data can remain private, and whether the government's methods in obtaining the information are overly intrusive.[12] Part III considers the

---

[8] *See* 18 U.S.C. § 2701 (2009).

[9] *Foreign Intelligence Surveillance Act (FISA) Part 1* (transcript on file with Federal Law Enforcement Training Centers), *available at* https://www.fletc.gov/audio/foreign-intelligence-surveillance-act-fisa-part-1-mp3 (last visited Jan. 6, 2015)
("During the Watergate scandal in the 1970s, Congress and the public learned that the privacy of some U.S. citizens had been invaded. Congress responded by developing the Foreign Intelligence Surveillance Act. FISA established that non-criminal electronic surveillances were only permissible for the purpose of collecting foreign intelligence. Second, the law identified who could be targeted for electronic surveillance—namely, foreign powers and agents of foreign powers. Third, the law set forth a probable cause standard that had to be met before electronic surveillance was allowed. Fourth, the Act established two Foreign Intelligence Surveillance Courts.").

[10] *See* 50 U.S.C. § 1804(a)(6)(B) (2010).

[11] 50 U.S.C. § 1881a (2008).

[12] *See infra* Part II.

SCA and FISA as applied to cloud data. Finally, Part IV analyzes the use of the special needs doctrine to justify the acquisition of data without probable cause and a warrant. The special needs doctrine is being used to authorize FISA's wide reach. The application of the special needs doctrine to national security investigations is an impermissibly overbroad use of this doctrine, since evidence from these investigations is being introduced in derivative prosecutions that are not based on national security.

Compared to other countries, the United States is an "outlier in relation to the global community" on privacy issues.[13] Other countries follow the European Union, which emphasizes privacy, safeguards and personal liberty.[14] As constitutional scholar Paul Ohm has pointed out, in the United States: "Current Fourth Amendment doctrine . . . places far fewer hurdles in front of the police when they use the fruits of somebody else's surveillance than when they do the surveillance themselves."[15] As the surveillance society expands, he continues, "the police will learn to rely more on the products of private surveillance," and become "passive consumers rather than active producers of surveillance."[16]

Protection for online data is unlikely to come from Congress.[17]

---

[13] Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623 (2012) (examining legal developments in the United States and the European Union). "Computing resources are now accessible globally, and the processing of personal information increasingly occurs through such distributed resources." *Id.* at 1629.

[14] *Id.* at 1636. The 2012 European Union Proposed Regulation on Data Protection "permits an international transfer of data from the European Union only if the Commission has made a finding of adequacy, use is made of 'appropriate safeguards,' or one of its enumerated exceptions applies to the transfer." *Id.* at 1637. In contrast, "U.S. information privacy law does not give government officials the power to block international transfers of personal information." *Id.* at 1636.

[15] Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1311 (2012).

[16] *Id.*

[17] Congress's approval of PRISM, which allows NSA officials to collect material including search history, contents of emails, stored data, file transfers, and live chats, illustrates that national security is foremost on Congress's agenda. *See* Jennifer Stisa Granick & Christopher Jon Sprigman, *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html ("The government justifies Prism under the FISA Amendments Act of 2008. Section 1881a of the act gave the president broad authority to conduct warrantless electronic surveillance. If the attorney general and the director of national intelligence certify that the purpose of the monitoring is to collect foreign intelligence information about any non-American individual or entity not known to be in the United States, the Foreign Intelligence

Instead, we should focus on *judicial* preservation of privacy in the area of cloud computing. Ohm states: "To save the Fourth Amendment, [judges] will transform it, abandoning the reasonable expectation of privacy test."[18] "[J]udges are not likely to lash the Fourth Amendment to the sinking ship of privacy."[19] Thus, courts must ensure that under appropriate circumstances data stored in the cloud receives protection under the Fourth Amendment.

Recent Supreme Court opinions suggest that government inspection of data in a secured cloud is a search. In *United States v. Jones*, Justice Alito, in his concurring opinion, indicated that society generally holds an expectation that law enforcement will not surreptitiously monitor our movements for a long period of time.[20] Justice Sotomayor, in her concurring opinion, commented, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[21] As she aptly noted, the third-party doctrine is not appropriate for the digital age.[22] In *City of Ontario, California v. Quon*, the Supreme Court indicated that it might be ready to find a reasonable expectation of privacy in ISP systems.[23]

In fact, the Supreme Court in *Riley v. California* recently held that police may not access digital information from any device seized from an individual during a lawful arrest without a warrant, unless exigent circumstances permit a reasonable warrantless search.[24] The *Riley* decision recognized an individual's right to digital privacy against the reach of the government. Today's cell phones, the Court said, hold the "privacies of life."[25] Because of the ubiquity of today's smart

Surveillance Court can require companies to provide access to Americans' international communications.").

See 50 U.S.C. § 1881a (2008) (outlining the procedures and limitations for targeting certain persons outside the United States, other than United States persons, for the purpose of obtaining foreign intelligence information).

[18] Ohm, *supra* note 15, at 1321.

[19] *Id.* at 1312.

[20] United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

[21] *Id.* at 957 (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting)); *see also* Katz v. United States, 389 U.S. 347, 351–52 (1967).

[22] *Jones*, 132 S. Ct. at 957.

[23] *See* City of Ontario, California v. Quon, 560 U.S. 746, 759–60 (2010).

[24] Riley v. California, 134 S. Ct. 2473 (2014).

[25] *Id.* at 2495 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

phones, their massive storage capacity to hold an almost unlimited amount of sensitive personal information, and the risk that a warrantless search would produce an unconstitutional invasion of privacy, the Court decided to extend Fourth Amendment protection to digital devices acquired during a lawful arrest.[26]

Going forward, the Court may well find that when a citizen voluntarily provides information for storage with a third-party ISP she has not relinquished her Fourth Amendment protections. After all, government inspection of this same information in another form would be considered a search. For example, the owner of a closed briefcase that is moved in the public domain from home does not give up her Fourth Amendment protection upon exiting her home.[27] The substitution of a third-party cloud facility for the briefcase should not alter the result. *Riley* appears to suggest that digital data deserve the same Fourth Amendment protections as a locked filing cabinet.[28]

There is a distinction between voluntary disclosure to dynamic third parties (like banks) and disclosure to nonhuman, passive, inactive ISP transmitters. Because nonhuman systems do not invade the privacy of their customers, they do not diminish it. Bank employees analyzing customer records (*Smith*) are different than automated ISPs, which do not "process" data or communications. Telephone companies, which transmit telephone numbers (*Miller*), can be distinguished from ISPs which store nonpublic content-based information. In *Riley*, the Supreme Court skirted the issue of how to regulate searches of digital data stored on cloud networks.[29] Instead of addressing the third-party doctrine, the Court analyzed the confiscation of Riley's phone and personal information by the police as a search incident to a lawful arrest.

The *Riley* opinion nudges the Court closer to the conclusion proposed by this article: the third-party doctrine should not apply to data stored on the cloud because the substance of the data remains the same, whether it is stored in a physical cabinet or in cyberspace. As legal commentator David A. Sklansky states, "In the long term, sensible interpretation of the Fourth Amendment will require the Court to . . .

---

[26] *Id.* at 2489–91.

[27] *See* United States v. Benitez-Arreguin, 973 F.2d 823, 828–29 (10th Cir. 1992) (finding that the bailee of a duffel bag had reasonable expectation of privacy in the bag and standing to challenge the search).

[28] *Riley*, 134 S. Ct. at 2489–91.

[29] The Court rejected the lower courts' proposals as overbroad. *Id.* at 2491–93.

abandon the assumption that anything knowingly exposed 'to the public' is therefore fair game for the police."[30] Or, perhaps the Court will decide that material stored in a cloud has not been "knowingly exposed."

A. What are Clouds?

"How do you catch a cloud and pin it down?"[31]

Though cloud data is intangible and its storage with a third party differs from traditional storage methods such as file cabinets and briefcases, its use is becoming essential for work and for personal participation in modern life. Cloud computing is the act of using global storage facilities to store information electronically and grant access to uploaded information using any electronic device from any location at any time.[32] In laymen's terms, the cloud is a network made of hundreds of thousands of servers that store data.[33] A user only needs a computer, tablet or smart phone connected to a cloud provider to network with remote servers and carry out tasks such as working in Google Drive or viewing personal photos.[34] Most technology experts expect that by 2020, individuals, businesses, and government entities will access data online. They predict that users will share and store information through remote server networks, rather than depend on information housed on personal and office computer hard drives.[35]

---

[30] David A. Sklansky, *Back to the Future: Kyllo, Katz, and Common Law*, 72 MISS. L.J. 143, 210 (2002).

[31] RICHARD RODGERS & OSCAR HAMMERSTEIN II, *Maria*, *on* THE SOUND OF MUSIC (Columbia Masterworks 1959).

[32] *See* Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. TECH. L. & POL'Y 229, 231–32 (2011); Jack Newton, *Ten Reasons to Adopt Cloud Computing for Your Law Office*, 74 TEX. B.J. 860, 860 (2011). With cloud computing, "rather than accessing software and data on desktop computers and servers located 'on premises,' you access your software and data via a web browser . . . [Y]our software and data are hosted and maintained by a third-party provider." *Id.*; *see also* Asit K. Mishra et al., *Towards Characterizing Cloud Backend Workloads: Insights from Google's Compute Clusters*, 37 ACM SIGMETRICS PERFORMANCE EVALUATION REV. 34, 34–35 (2010) (noting that Google's Cloud is "the largest cloud backend on the planet" and that "tens of thousands of tasks execute daily on Google computer clusters.").

[33] *See* Harshbarger, *supra* note 32; Newton, *supra* note 32; Mishra et al., *supra* note 32.

[34] *See* Harshbarger, *supra* note 32; Newton, *supra* note 32; Mishra et al., *supra* note 32.

[35] Some experts believe "that for many individuals the switch to mostly cloud-based work has already occurred, especially through the use of browsers and social

Individuals and businesses rely upon anonymous and passive third-party ISPs to efficiently process and access online data. Non-negotiable user agreements are required by most ISPs before subscribers can sign up for storage accounts. These contracts complicate privacy issues because they are difficult for most people to understand and force users to choose between relinquishing many rights they may possess in their information and foregoing the use of the service.[36]

For example, Apple's recently updated privacy policy requires iCloud users to acknowledge and agree that Apple is permitted to disclose account information and content to law enforcement authorities and government officials if Apple believes "disclosure is necessary or appropriate."[37] Google says, "We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to . . . meet any applicable law, regulation, legal process or enforceable governmental request."[38] Such agreements operate as a waiver of privacy for governmental use, usually without user knowledge or ability to decline.[39]

networking applications." *Responses to a Tension Pair on the Likely Future of Cloud Computing*, ELON UNIVERSITY SCHOOL OF COMMUNICATIONS, http://www.elon.edu/e-web/predictions/expertsurveys/2010survey/future_cloud_computing.xhtml (last visited Jan. 6, 2015).

[36] *See* Robert Gellman & World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM (Feb. 23, 2009), http://www.worldprivacyforum.org/www/wprivacyforum/pdf/WPF_Cloud_Privacy_Report.pdf (discussing the relevance of a provider's terms of service to privacy and confidentiality protections).

[37] *Privacy Policy*, APPLE, INC., http://www.apple.com/legal/privacy/en-ww (last updated Sept. 17, 2014) ("It may be necessary — by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence — for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.").

It is interesting to note that Apple's revised privacy policy now asks users to "choose a region" and a country. *See Apple Customer Privacy Policy*, APPLE, INC., http://www.apple.com/legal/privacy (last visited Jan. 6, 2015).

[38] *Privacy Policy*, GOOGLE, INC., http://www.google.com/policies/privacy (last updated Mar. 31, 2014).

[39] User agreements may be unenforceable in accordance with tenancy and bailment principles. Fourth Amendment interests can be at stake when law enforcement seizes private information from bailees or landlords. Landlords cannot consent to government

Several ISP user agreements say they protect user information from easy government access. Wuala, a company specializing in cloud

searches without a warrant even if language permitting them to do so is included in a rental agreement. *See* Chapman v. United States, 365 U.S. 610, 616 (1961); *see also* Ferguson v. State, 488 P.2d 1032, 1035–36 (Alaska 1971); Commonwealth v. Gutierrez, 750 A.2d 906, 909 (Pa. Super. 2000); Commonwealth v. Basking, 970 A.2d 1181, 1189 (Pa. Super. 2009).

Applying a landlord/tenant comparison, an end user license agreement is a tenancy—the users are the tenants, the ISPs are the landlords and the ISPs' servers are the property. An ISP as landlord, by virtue of a user agreement, would be unable to consent to a search of a person's cloud without a warrant. Tenant users would have the right to object to warrantless government searches of their data. *See Chapman*, 365 U.S. at 616–17; s*ee also* David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2237 (2009) ("[A] service provider is not a party to the contents any more than a landlord is a party to what goes on behind this tenants' closed doors due to his limited right of entry.").

Employing a bailment analogy, the users are the bailors, the ISPs are the bailees, and the clouds are the bailed property. Bailees have a duty to object to warrantless government searches regardless of inapposite user agreements. United States v. Perea, 986 F.2d 633, 640 (2d Cir. 1993).

A cloud can be analogized to a bailment. Like a personal storage agreement, the user and the ISP electronically sign a contract. The ISP is in possession of the information uploaded for the specific term of storage, with no independent rights to the information. By entering into an agreement with an ISP to store documents in the cloud, an individual places his documents in the ISP's care, with the understanding that the ISP will make the documents available at a place of his or her choosing. By relinquishing these documents, the user/bailor loses his privacy interests under *United States v. Rawlings*. *See* United States v. Rawlings, 448 U.S. 98, 106 (1980). Under an ISP as bailee theory, an ISP could object to a government search. *See Perea*, 986 F.2d at 640; United States v. Benitez-Arreguin, 973 F.2d 823, 829 (10th Cir. 1992); *see also* State v. Shelton, 191 P.3d 420, 423 (Mont. 2008).

The U.S. Court of Appeals for the Sixth Circuit in *United States v. Warshak* applied both bailment and tenancy analogies. United States v. Warshak, 631 F.3d 266, 287–88 (6th Cir. 2010) (quoting Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, U. CHI. LEGAL F. 121, 165 (2008)).

If acceptance of an ISP user agreement confers rights on the provider to access the contents of the account and consent to a law enforcement search, there is no privacy in electronic communications, transactions and Internet usage. At this time, however, the third-party doctrine renders application of tenancy and bailment laws to user agreements unnecessary because it signifies that users have no expectation of privacy due to the presence of the third-party ISP. In addition, the SCA and FISA make application of tenancy and bailment laws to user agreements unnecessary, as these statutes require ISPs to surrender data. Courts have not found end user licensing agreements unenforceable or imposed a duty on the part of ISPs to defend privacy or let users know when the government asks for data.

storage, claims "secure storage for your files." Its terms of service provide, "all files you store . . . will be encrypted such that they can neither be read by [us] nor by any third party, unless the data is explicitly shared or made public by you. [Our company] has no access to your password, does not know it and cannot reset or recover it."[40] Dropbox is a company that allows users to save and share documents, photos, and files in the cloud.[41] Its terms of service provide, "You retain full ownership to your stuff. We don't claim any ownership to any of it."[42] It is unlikely that these consumer friendly agreements can stop the government from acquiring user data. Existing statutory protection covers "communications" and may not apply if the materials sought by the government are stored files or documents.[43]

Existing statutes, FISA and the SCA, provide timely examples of waiver of privacy and secrecy.[44] The FISA Amendments Act of 2008 (FAA), for example, allows the NSA to obtain certain communications without having to request them from an ISP or obtain individual court orders.[45] The SCA permits the government to obtain the contents of

---

[40] *Wuala Terms of Service*, LACIE, http://www.wuala.com/en/about/terms (last visited Jan. 6, 2015).

[41] *The Dropbox Tour*, DROPBOX, https://www.dropbox.com/tour (last visited Oct. 17, 2014).

[42] *Dropbox Terms of Service*, DROPBOX, https://web.archive.org/web/20140101095409/https://www.dropbox.com/terms (accessed by inserting "https://www.dropbox.com/terms" into Internet Archive search engine and accessing January 1, 2014 archive).

[43] 18 U.S.C. § 2702 (2008) (prohibiting persons or entities that provide electronic communication services or remote computing services to the public from knowingly divulging contents of users' communications, except in limited circumstances). Users receive the "benefit" of the more protective user agreements only if they choose to subscribe to these companies, which provide limited storage services, unlike Apple or Google, both full-service companies.

[44] 50 U.S.C. § 1805(c)(2)(B) (2010) (providing that when a carrier, or ISP, is directed to furnish the government with the facilities and information needed to conduct the electronic surveillance, the carrier or ISP does so "in such a manner as will protect its secrecy"); *see* 50 U.S.C. § 1805(c)(2)(C) (2010) (requiring the carrier to "maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records containing the surveillance or the aid furnished that such [carrier] wishes to retain").

[45] *See* 50 U.S.C. § 1881a (2008) ("[T]he Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year. . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information," subject to certain limitations.); *see also* Glenn Greenwald & Ewen MacAskill, *NSA PRISM Program Taps in to User Data of Apple, Google and*

Americans' data and communications without probable cause and denies the user and the ISP the ability to refuse access to the government.[46] The rise of cloud computing raises new questions about the application of these statutes and whether government acquisition of electronic data is a Fourth Amendment seizure.

II. THE THIRD-PARTY DOCTRINE AND CLOUD-BASED DATA

"But now they only block the sun"[47]

The third-party doctrine, exempting information from Fourth Amendment protections, should not apply to data stored in the cloud. In the landmark case of *Katz v. United States*, the Supreme Court broadened its definition of what constitutes a search to account for technological advancements by holding that the Fourth Amendment protects intangible interests.[48] The case involved the government placing an electronic recording device on the outside of a public telephone booth to record Katz's conversation. The Court posited that in order for a search to occur an individual must possess an actual expectation of privacy in the thing searched and that expectation must be one that society recognizes as reasonable.[49] This two-pronged approach rejected the traditional standard, articulated in *Olmstead* v. *United States*, that a physical intrusion was necessary to trigger a Fourth Amendment violation.[50] In the absence of a physical trespass, this decision remains the standard for determining whether a Fourth Amendment violation has occurred.[51]

Others, THE GUARDIAN (June 6, 2013, 3:23 PM), http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

[46] 18 U.S.C. § 2703 (2009).

[47] JONI MITCHELL, *Both Sides, Now*, *on* CLOUDS, (Reprise Records 1969).

[48] Katz v. United States, 389 U.S. 347 (1967).

[49] *Id.* at 348, 361 (Harlan, J., concurring). The approach outlined in Justice Harlan's concurring opinion became the standard applied in Fourth Amendment cases. *See infra* note 51.

[50] *Id.* at 352–53; *see* Olmstead v. United States, 277 U.S. 438, 457, 464, 466 (1928).

[51] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33–38 (2001) (holding that because the agents failed to procure a warrant before using a thermal imaging device to peer into the "sanctity of the home," the Court found an unlawful search); Minnesota v. Carter, 525 U.S. 83, 90–91 (1998) (police officer's observation through closed blinds of the defendants bagging cocaine in another's apartment did not violate the Fourth Amendment because the defendants had no reasonable expectation of privacy when they were in apartment for only a few hours and solely for a business transaction); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (finding that police officers'

Applying *Katz* to the modern world of cloud computing can be difficult. However, there can be a reasonable expectation of privacy in data stored in the cloud. Sensitive and personal information, such as tax returns and personal and business correspondence, used to be stored in a person's home or office in a physical form. Later, it was housed on personal and office computers. Now this data, which reveals a startling amount of intimate information that can generate a precise, comprehensive record of an individual's life, has drifted to the cloud.[52] An ISP's ability to access this material should not diminish one's personal liberty. Yet, the third-party doctrine states that when a person voluntarily gives information to a third party, even for a limited, specific purpose, and that third party delivers the information to law enforcement, the government's acquisition of the information cannot be defined as a search.[53]

The doctrine was established in *United States v. Miller*. In *Miller*, the police presented the defendant's banks with subpoenas to produce records of his accounts.[54] The banks, without informing the defendant of the subpoenas or requesting permission from the defendant,

warrantless visual observations from a plane flying in navigable airspace of marijuana plants in the defendant's backyard did not violate the Fourth Amendment); United States v. Knotts, 460 U.S. 276, 280–81 (1983) (finding that government's warrantless monitoring of a beeper to track a subject's movements in public did not constitute a search because all of the information gathered from the beeper could have been procured by visual surveillance of the automobile in which he was traveling).

However, in 2012 the Court decided, on a trespass rationale, that the government's insertion of a Global Positioning System (GPS) and tracking of a vehicle on the public streets did constitute a search. United States v. Jones, 132 S. Ct. 945, 949 (2012). In *United States v. Jones*, the Court explained, "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *Id.* at 952; *see also* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

[52] *See* Gellman, *supra* note 36 (discussing how the third-party doctrine applies to privileged information stored on the cloud).

[53] *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *see also* United States v. Smith, 442 U.S. 735, 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[54] *Miller*, 425 U.S. at 437–38.

provided law enforcement with the requested records.[55] The Court, adopting an assumption of the risk rationale, stated that a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[56] Finding that the defendant had no privacy interest in his records once he voluntarily revealed such information to his banks, the Court held that it was constitutional for the banks to deliver the information to the government, regardless of the fact that the material was revealed by the defendant under the assumption that it would be used for a limited purpose.[57]

Three years later, in *Smith v. Maryland*, the Supreme Court held that the installation and use of a pen register on the defendant's telephone to record the numbers he dialed without a warrant did not constitute a search under the Fourth Amendment.[58] Adopting the *Miller* analysis, the Court found that the defendant's use of the telephone company's services, and the resulting exposure of that information to the phone company and its employees, demonstrated that he "assumed the risk" that the company or its employees would disclose the numbers he dialed to the police.[59] In distinguishing the facts from those of *Katz*, the Court reasoned that because a pen register only records numbers dialed and not the contents of communications, the only way its installation could be considered a search is if the defendant had a legitimate

---

[55] *Id.* at 438. The banks ultimately provided the agents with copies of the defendant's deposit slips, checks, financial statements and monthly balance statements. *Id.*

[56] *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).

[57] *Id.* Many state courts have determined that their respective state constitutions provide greater privacy for bank records than the Fourth Amendment. *See, e.g.*, Charnes v. DiGiacomo, 612 P.2d 1117, 1121, 1124 (Colo. 1980) (en banc) (finding that, under the Colorado Constitution, individuals have a reasonable expectation of privacy in their bank records); Winfield v. Div. of Pari-Mutuel Wagering, Dep't of Bus. Regulation, 477 So. 2d 544, 548 (Fla. 1985) (finding that the Florida Constitution "recognizes an individual's legitimate expectation of privacy in financial institution records"); People v. Nesbitt, 938 N.E.2d 600, 604–05 (Ill. App. Ct. 2010) (finding that the Illinois Constitution provides greater protection for the privacy of bank records than "the protections offered by the federal constitution"); Commonwealth v. DeJohn, 403 A.2d 1283, 1291 (Pa. 1979) (finding that Article 1, Section 8 of the Pennsylvania Constitution establishes that individuals have "a legitimate expectation of privacy in records pertaining to their affairs kept at a bank"); State v. Thompson, 810 P.2d 415, 418 (Utah 1991) (finding that, under the Utah Constitution, individuals have a reasonable expectation of privacy in their banking records).

[58] *Smith*, 442 U.S. at 737, 745–46.

[59] *Id.* at 744.

expectation of privacy in the numbers he dialed on his telephone.[60]

Miller and *Smith* loosened the definition of a search, paving the way for government license to monitor an individual through digital technologies. The third-party doctrine has been used as the legal basis for the government's easy access to information stored by individuals or businesses contracting with third-party ISPs.[61] It has also been applied by lower courts to deny Fourth Amendment protection to historical cell-site data held by third-party cellular telephone providers, allowing law enforcement to infer the physical location of a cell phone user.[62] On the

[60] *Id.* at 741 ("[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."). Nine years later, in *California v. Greenwood*, the Court found that "respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector." California v. Greenwood, 486 U.S. 35, 40 (1988).

[61] *See, e.g.*, United States v. Skinner, 690 F.3d 772, 774–77 (6th Cir. 2012) (finding that, because Skinner lacked a reasonable expectation of privacy in the information emitted from his pay-as-you-go cellular phone, there was no Fourth Amendment search when the government used the GPS feature on the phone to obtain real-time location information); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (finding that, although individuals have a reasonable expectation of privacy in their home computers, that expectation is diminished once information is transmitted over the Internet or email and received by a third person); United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *11 (D. Ariz. May 8, 2013) ("[F]ederal courts consistently rely on *Smith* and *Miller* to hold that defendants have no reasonable expectation of privacy in historical cell-site data because [they] voluntarily convey their location information to the [provider] when they initiate a call and transmit their signal to a nearby cell tower and because the companies maintain that information in the ordinary course of business."); United States v. Wilson, No. 1:11–CR–53–TCB–ECS–3, 2012 WL 1129199, at *7 (N.D. Ga. Feb. 20, 2013) (third-party doctrine is applicable to historical cell site information); United States v. Madison, No. 11–60285–CR, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012) ("Just as the *Smith* petitioner's actions of making telephone calls provided information to the petitioner's telephone company, Defendant knowingly and voluntarily gave information to his communications-service provider that he was located within the range of specific cell towers at the times that he made and received telephone calls on his cell phone.").

[62] *See, e.g.*, *In re* Application of United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (finding that court orders authorized by the SCA to compel cell phone service providers to produce the historical cell site information of their subscribers are not per se unconstitutional); United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012) (noting that although some courts have considered the length of time the government acquired historical cell site location data, a majority of courts have concluded that governmental acquisition of such data "pursuant to the Stored Communications Act's specific and articulable facts standard does not implicate the Fourth Amendment, regardless of the time period involved").

basis of the third-party doctrine, lower courts also have denied Fourth Amendment protection to stored Internet Protocol (IP) address information, the unique string of numbers that identifies each device attached to the Internet.[63] Fourth Amendment protection has also been withheld from computer files voluntarily made available over a closed, peer-to-peer file-sharing program commonly used to access media files such as books and music.[64]

Although some courts have applied the third-party doctrine to emerging technologies, not all courts have followed this approach. Many state statutes and several federal courts have rejected the third-party doctrine or found a way to distinguish it; legal commentators have also been critical of it.[65]

---

[63] *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703, 830 F. Supp. 2d. 114, 133 (E.D. Va. 2011) (finding that even if petitioners had a reasonable expectation of privacy in their IP addresses, they voluntarily conveyed that information to Twitter in order to use Twitter's services, extinguishing any Fourth Amendment protection under the third-party doctrine).

[64] United States v. Sawyer, 786 F. Supp. 2d 1352, 1356 (N.D. Ohio 2011). Although the defendant's shared files over a closed file-sharing network were accessible only to his friends, he had no objectively reasonable expectation of privacy. *Id.* The third-party doctrine applied to open file-sharing networks, accessible to the public. *Id.* Even though the defendant may have had a *more* reasonable expectation of privacy in his files than someone who shared his files publicly, that expectation is still not one that is objectively reasonable. *Id.* Once the defendant granted access to his friends, "he had no control over the manner in which his friends used that access." *Id.*

[65] In *Beauford*, the Pennsylvania appellate court rejected the reasoning in *Smith* and held that under Article 1, Section 8 of the Pennsylvania Constitution, police must make a showing of probable cause and obtain a warrant before attaching a pen register to a person's telephone line, extending the Pennsylvania Supreme Court's decision in *DeJohn*, which held that police must obtain a warrant in order to obtain an individual's banking records. Commonwealth v. Beauford, 475 A.2d 783, 788–89, 791 (Pa. Super. 1984). "For all practical purposes an individual in America today has very little choice about whether the telephone company will have access to the numbers he dials and the frequency of times he dials them. The company has a virtual monopoly over vital communications media." *Id.* at 789.

In *Warshak*, the court held that the third-party doctrine did not extinguish the defendant's reasonable expectation of privacy in his emails even though they were sent and received through a third-party ISP. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). The court distinguished *Miller*, which "involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue here." *Id.* The court found that the defendant in *Miller* conveyed the information for the bank's use in the "ordinary course of business," whereas here, in the case of emails, the third party was not the "intended recipient of the emails," but merely an intermediary. *Id.* The court concluded that, just as letters are

It is time to reconsider the notion that an individual has no reasonable expectation of privacy for information voluntarily disclosed to third parties for the limited purpose of storage.[66] As an example,

protected from government intrusion as they pass through the postal service, emails are protected from government intrusion as they pass through a third-party ISP. *Id.* at 285–86. *See also In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (holding that cell site location information (CSLI) is not automatically denied constitutional protection because of its inadvertent disclosure to third-party cellular service providers); *see also* State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (finding that, under New Jersey Constitution Article 1, Paragraph 7, individuals have a reasonable expectation of privacy in the location of their cell phones. Individuals can reasonably expect that the personal information they provide to third-party providers will remain private); H.B. 603, 2013 Leg., 63rd Sess. (Mont. 2013) (effective October 1, 2013) (to be incorporated into Title 46 [Criminal Procedure], Ch. 5 [Search and Seizure]); MONT. CODE ANN. § 46-5-110 (police cannot obtain cell phone location information without obtaining a warrant).

See also Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1 (2013) (arguing that interpersonal privacy concepts should apply to social networking relationships over the Internet and provide a better way to apply the "reasonable expectation of privacy" test because these concepts avoid the problems associated with the application of the third-party doctrine); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007) (arguing that courts should review the facts on a case-by-case basis and not apply a bright-line rule).

[66] ISP private-party user agreements are typically drafted to comply with the third-party doctrine. *See supra* note 61. If the third-party doctrine did not apply, user privacy concessions in cloud computing agreements would be unnecessary, as ISPs would not be required to disclose this information to the government.

Orin S. Kerr states, "The breach of Terms of Service should not eliminate a reasonable expectation of privacy in an Internet account for the same reasons that the breach of a rental agreement in an apartment does not itself eliminate a tenant's reasonable expectation of privacy." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1031 n.100 (2010). However, "agreeing to Terms of Service may in some cases confer rights on the provider to access the contents of the account or consent to a law enforcement search." *Id.* Kerr states that "[t]he difference between elimination of a reasonable expectation of privacy and consent can be an important one because consent is bounded by the scope of consent whereas elimination of a reasonable expectation of privacy eliminates all Fourth Amendment rights in the information." *Id.*

The U.S. Court of Appeals for the Sixth Circuit, in *United States v. Warshak*, recognized the consent issue raised by Kerr but stated: "While we acknowledge that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account, we doubt that will be the case in most situations, and it is certainly not the case here." *Warshak*, 631 F.3d at 286

assume the government serves Apple with a subpoena to access a pornographic video stored on a United States citizen's iCloud account for more than a year. Pursuant to the third-party doctrine, an overwhelming number of courts have held that individuals have no reasonable expectation of privacy in information voluntarily disclosed to an ISP. Thus, government acquisition of the video is not a Fourth Amendment seizure[67] and neither the SCA nor the FISA provide sufficient statutory protection for this material.[68]

In contrast, assume the same citizen copies the video on to the hard drive of her computer and creates a DVD, which she stores in a file cabinet in her home. To access the video from the computer hard drive or the DVD, the government would be required to obtain a warrant supported by probable cause.[69] The outcome should be the same and the same standard should apply whether the video is stored in the cloud, computer hard drive or on a DVD.

A. The Inhuman ISP

In cloud computing, an ISP is merely a conduit that receives and stores information, rather than an active participant. An ISP server containing data is merely a place to hold information, a means to an end. The data is generated automatically by the network, conveyed to the provider not by human hands, but by invisible technology.[70] Information

(internal citations omitted).

[67] United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008).

[68] *See infra* Part III; *see, e.g., In re* Application of United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012); *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).

[69] For example, in *O'Connor v. Ortega*, the Supreme Court found a reasonable expectation of privacy in a doctor's office file cabinets and desk that he did not share. O'Connor v. Ortega, 480 U.S. 709, 718–19 (1987). In *United States v. Simons*, the Fourth Circuit found a reasonable expectation of privacy in the contents of a person's hard drive. United States v. Simons, 206 F.3d 392, 399 (4th Cir. 2000). *See also* Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002) ("If the employer equips the employee's office with a safe or file cabinet or other receptacle in which to keep his private papers, he can assume that the contents of the safe are private.").

[70] *See In re* Application of United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010), *rev'd*, 724 F.3d 600 (5th Cir. 2013); David S. Cox, *Cloud Computing — The Invisible Revolution*, MICROSOFT FIN. SERVS. BUS. TALK (Feb. 4,

voluntarily disclosed to this automated "third party" should not, for this reason alone, be stripped of Fourth Amendment protection.

Orin Kerr believes that "the third-party doctrine has not been extended to intermediaries that merely send and receive contents without needing to access or analyze those communications."[71] Constitutional law scholar Matthew Tokson states, "while users perceive disclosure of their personal information to humans as a serious privacy harm, they do not consider disclosure to automated systems alone to be a significant harm."[72] Automated systems do not invade privacy and thus do not diminish it. Or, we can look at it as Ohm suggests and say the *Katz* test should not apply because the third-party doctrine allows the police to rely "on the products of private surveillance" and passively diminish our personal liberties.[73]

B. Users Have No Choice

As technology advances and becomes essential to complete ordinary tasks, alternatives to cloud computing will become obsolete. In the near future, individuals and businesses will have little choice but to rely on anonymous ISPs to process and access data efficiently.[74] Yet the third-party doctrine's premise—that by "voluntarily" sharing their information with ISPs, users have assumed the risk that the government will seize it—precludes those users from Fourth Amendment protection for this data. In determining whether data stored in the cloud should be entitled to Fourth Amendment protection, it is appropriate to consider whether refraining from the use of an ISP's services would preclude an

2011, 3:52 AM), http://blogs.msdn.com/b/businesstalk/archive/2011/02/04/cloud-computing-the-invisible-revolution.aspx. Many new technologies are invisible. *Id.* ("[I]n the future, we will look at a device and not realize it is a computer, because its computing power will be based in the cloud."). *Id. See also* Couillard, *supra* note 39, at 2237 ("[T]he provider is merely providing a platform for using and storing the content via the cloud."). Couillard states, "A service provider, even if it has the capacity of accessing the contents of an email, is not a party to the information." *Id.*

[71] Kerr, *supra* note 66, at 1038.

[72] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 611–12, 621 (2011).

[73] Ohm, *supra* note 15, at 1338; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[74] Fourth Amendment scholar Wesley MacNeil Oliver added, "[t]o do business, or be social, we must use technology not yet protected from the government's prying eye." Wesley MacNeil Oliver, *Western Union, The American Federation of Labor, Google, and the Changing Face of Privacy Advocates*, 81 MISS. L.J. 971, 986 (2012).

individual or business from meaningful participation in society and the economy.

In *City of Ontario, California v. Quon*, eight justices indicated that they might be ready to find a reasonable expectation of privacy in ISP systems, even though they travel through third-party servers.[75] As Justice Kennedy wrote, "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy," even though those communications pass through public spaces.[76]

Justice Brennan, in his dissenting opinion in *United States v. Miller*, stated that the disclosure by individuals or businesses of their "financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[77] An ISP account today is similar to what a bank account was in 1976. It is becoming impossible to participate in the economic life of contemporary society without maintaining an ISP account.

The United States Court of Appeals for the Sixth Circuit refused to apply the third-party doctrine to emails sent through an ISP, holding that they are not "voluntarily" conveyed by the subscriber for an ISP's use.[78] With data stored in the cloud, a user is even more likely to retain a reasonable expectation of privacy because unlike an email, data is not a communication and a knowing and voluntary disclosure is more doubtful.[79]

Unlike records disclosed to banks for processing by bank employees, users do not choose to share their personal information with an ISP. The Supreme Court of New Jersey recently held that "cell-phone

---

[75] City of Ontario, California v. Quon, 560 U.S. 746, 759–60 (2010).

[76] *Id.*; *see also* Riley v. California, 134 S. Ct. 2473 (2014).

[77] United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

[78] United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[79] *See* Chris Hoffman, *Ten Ridiculous EULA Clauses That You May Have Already Agreed To*, MAKEUSEOF (Apr. 23, 2012), http://www.makeuseof.com/tag/10-ridiculous-eula-clauses-agreed ("Let's be honest, no one reads EULA's (End User Licensing Agreement) — we all just scroll down to the bottom and click 'I Accept'. EULAs are full of confusing legalese to make them incomprehensible to the average person . . . the enforceability of EULAs is generally controversial, and some of these clauses would likely be tossed out by a judge, even if EULAs were legally enforceable.").

users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone."[80] When an ISP, without user notice or consent, grants the government access to a user's personal and private information, the user should be entitled to Fourth Amendment protection of that information.

C. Only the Location Has Changed

As previously discussed, private data secured with a user name and password is analogous to papers located in a file cabinet, briefcase or third-party storage facility.[81] The law is very clear that an individual possesses an expectation of privacy in the contents of a personal office, as well as a shared office with a locked desk and file cabinet, even if the employer has a master key.[82] Similarly, a closed briefcase that is moved in the public domain from home, to office, to court is entitled to Fourth Amendment protection.[83] Similarly, hard copies of documents stored in

---

[80] State v. Earls, 70 A.3d 630, 641 (N.J. 2013).

The United States Court of Appeals for the Fifth Circuit, however, reached a different conclusion, stating "[a] cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call." *In re* Application of United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013). The court stated that the "Government does not require a member of the public to own or carry a phone." *Id.* at 613. The Fifth Circuit declined to reconsider this holding after *Riley*. United States v. Guerrero, 768 F.3d 351 (5th Cir. 2014). Noting "that the Supreme Court may . . . reconsider the third party doctrine in the context of historical cell site data or some other new technology," the Fifth Circuit quoted Barry Friedman: "'Those who believe the justices will leap from *Riley* to overturning the third party doctrine are dreaming.'" *Id.* at 360.

[81] *See* Couillard, *supra* note 39, at 2209 ("[C]ontainers satisfying the Katz test are usually subject to Fourth Amendment protection.") (citing Bond v. United States, 529 U.S. 334, 338–39 (2000) and Doe *ex rel* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 351, 353 (8th Cir. 2004)); *see also* State v. Reid, 945 A.2d 26, 28 (N.J. 2008) ("[C]itizens have a reasonable expectation of privacy, protected by Article I, Paragraph 7, of the New Jersey Constitution, in the subscriber information they provide to [ISPs]").

[82] *See* Morale v. Grigel, 422 F. Supp. 988, 999 (D.N.H. 1976) (finding that student resident contract that authorized entry by state university officials for minimal health and safety inspections did not authorize state university officials to search dorm room for stolen goods without a warrant); People v. Postall, 580 N.Y.S.2d 975, 979–980 (N.Y. Crim. Ct. 1992) (finding that post office regulation that left employee lockers subject to search did not constitute blanket consent on the part of employees to otherwise baseless searches of their personal lockers).

[83] *See* United States v. Benitez-Arreguin, 973 F.2d 823, 828–29 (10th Cir. 1992)

third-party storage areas are entitled to constitutional protection.[84] Because cloud-based data carry digital locks analogous to the physical locks on storage cabinets or briefcases, private data stored securely in the cloud should be inaccessible to the government.[85] One commentator has compared tangible to virtual containers, suggesting that "virtual concealment" by password protection and encryption satisfies the *Katz* subjective expectation of privacy prong.[86]

The Florida Supreme Court compared cell phones to desks and file cabinets and held that a law enforcement officer was not authorized to search the cell phone of an arrestee without a warrant.[87] The court

(finding that the bailee of a duffel bag had reasonable expectation of privacy in the bag and standing to challenge the search). One commentator believes even an unlocked container may be afforded Fourth Amendment protection if its contents are reasonably concealed. *See* Couillard, *supra* note 39, at 2210.

[84] *See* United States v. Johnson, 584 F.3d 995, 1001 (10th Cir. 2009) ("People generally have a reasonable expectation of privacy in a storage unit, because storage units are secure areas that 'command a high degree of privacy.' . . . an individual can have a recognized privacy expectation in a storage space even when he or she is not the lessee of the unit.") (internal citations omitted); United States v. Lnu, 544 F.3d 361, 365 (1st Cir. 2008) ("When evaluating whether a person has a reasonable expectation of privacy [in rented storage areas or units], courts examine a variety of factors, such as ownership of the premises, possession, access or control, ability to control or exclude others, and legitimate presence on the premises at the time of the search.") (citing United States v. Cardona–Sandoval, 6 F.3d 15, 21 (1st Cir. 1993)). An individual retains an expectation of privacy so long as a court finds that, in consideration of all of the factors, he has a reasonable expectation of privacy in the area. *Id.* at 366.
See also Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?* (Vanderbilt Univ. Law Sch., Working Paper No. 10-64, 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1734755.

[85] *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("[I]f government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception."); *see also* Steven R. Morrison, *What the Cops Can't Do, Internet Providers Can: Preserving Privacy in Email Contents*, 16 VA. J.L. & TECH. 253 (2011) (suggesting a four-part approach for courts and legislatures that would protect individual privacy interests while allowing ISPs to retain control over their networks and services).

[86] Couillard, *supra* note 39, at 2218. Couillard cites *United States v. D'Andrea*, where the federal district court analogized a website to a closed container in which records can be stored. *See* United States v. D'Andrea, 497 F. Supp. 2d 117, 118 (D. Mass. 2007).

[87] Smallwood v. State, 113 So. 3d 724, 740 (Fla. 2013) ("[W]hile law enforcement officers properly separated and assumed possession of a cell phone from Smallwood's person during the search incident to arrest, a warrant was required before the information, data, and content of the cell phone could be accessed and searched by law

found that permitting the government to search a cell phone without a warrant is analogous to "providing law enforcement with a key to access the home of the arrestee."[88] The United States Supreme Court echoed this ruling in *Riley* when it held that police must get a warrant before searching a cell phone seized incident to an arrest.[89]

Individuals and businesses are routinely drafting and storing highly sensitive and private documents in ISP systems in replacement of traditional storage methods. A document stored in the cloud could have been prepared originally on a word processor, printed, and placed in a file cabinet and later scanned and stored in the cloud.[90] Although material in the cloud is intangible and occasionally taken intentionally into the public domain (such as by opening a document at a public library), it should be deemed a "constitutionally protected space" and granted "some sort of Fourth Amendment oversight."[91]

III. GOVERNMENT ACQUISITION OF ELECTRONIC DATA IS A FOURTH AMENDMENT SEIZURE; GOVERNMENT INSPECTION OF DATA IN A CLOUD IS A FOURTH AMENDMENT SEARCH

"Dark clouds follow me everyway I go
Oh man, these blues got a hold on me"[92]

Supreme Court decisions addressing electronic devices provide a workable framework for balancing liberty and competing government needs. This precedent dictates that government acquisition of electronic data is a Fourth Amendment seizure.[93] Six factors, derived from these

enforcement.").

[88] *Id.* at 738 ("Physically entering the arrestee's home office without a search warrant to look in his file cabinets or desk, or remotely accessing his bank accounts and medical records without a search warrant through an electronic cell phone, is essentially the same for many people in today's technologically advanced society.").

[89] *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014).

[90] *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 718–19 (1987); Muick v. Glenayre Electronics, 280 F.3d 741, 743 (2002); U.S. v. Simons, 206 F.3d 392, 399 (2000). *But see* Kelly v. State, 77 So. 3d 818, 823 (Fla. Dist. Ct. App. 2012) (finding no reasonable expectation of privacy in an office shared with another employee).

[91] *See* United States v. Karo, 468 U.S. 705, 715–16 (1984) ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."); *see also* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19 (2008).

[92] CANNED HEAT, *Dark Clouds*, *on* BOOGIE 2000 (Ruf Records 1999).

[93] *See* United States v. Jones, 132 S. Ct. 945 (2012); Kyllo v. United States, 533 U.S.

decisions and set forth below, are relevant in determining whether the presumption should be rebutted.[94]

A. Nonpublic Information

The Fourth Amendment applies to invasions of privacy outside the home, "on the public roads," visible to all.[95] Nonpublic cloud data is not in the public domain; it is wholly private, for "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[96]

Precedent supports this stronger presumption of privacy. In *Katz*, the Court said that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[97] Further,

27 (2001); *Karo*, 468 U.S. 705; United States v. Knotts, 460 U.S. 276 (1983); Katz v. United States, 389 U.S. 347 (1967); *see, e.g.*, *In re* U.S. Application for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 117 (E.D.N.Y. 2011) ("Read together, *Karo* and *Knotts* stand for the proposition that the Government's obtaining of some electronically collected location information constitutes a search under the Fourth Amendment depending on the location (*Karo*) and, potentially, quantity (*Knotts*) of that information.").

[94] One other factor, unsupported by Supreme Court jurisprudence, should be considered. Before the government can obtain the contents of material stored in the cloud by an ISP, it should be required to demonstrate that its use of the data is consistent with the purpose for which it was released. State v. McAllister, 875 A.2d 866, 874 (N.J. 2005) ("[A] bank customer may not care that employees of the bank know a lot about his financial affairs, but it does not follow that he is indifferent to having those affairs broadcast to the world or disclosed to the government.") (quoting RICHARD A. POSNER, THE ECONOMICS OF JUSTICE (1981)). The government should be required to demonstrate that its use of the data it receives from the ISP is consistent with the limited purpose for which the individual or business shared it with the ISP. *Id.*; *see also* State v. Hunt, 450 A.2d 952, 956 (N.J. 1982) (recognizing a reasonable expectation of privacy in long distance telephone toll records because they were disclosed to the telephone company for a limited business purpose and not to other persons for other reasons).

[95] *Katz*, 389 U.S. at 351 ("For the Fourth Amendment protects people, not places."). *See Jones*, 132 S. Ct. 945, 949–53 (2012) (finding that situations "involving merely the transmission of electronic signals without trespass . . . *remain* subject to *Katz* analysis."); *see also* United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) ("A person does not leave his privacy behind when he walks out his front door, . . . [O]utside the home, the Fourth Amendment . . . secur[es] for each individual a private enclave, a 'zone' bounded by the individual's own reasonable expectations of privacy.") (internal quotation omitted).

[96] *See Katz*, 389 U.S. at 351.

[97] *Id.* at 359. Fourth Amendment scholar David A. Sklansky states: "[T]he privacy protected in Katz attached neither to a person (Charles Katz), nor to a place (the

in *United States v. Knotts*, the Court held that the government's use of a beeper to track the defendant while he was traveling "in an automobile on public thoroughfares" did not violate the Fourth Amendment because the defendant had "no reasonable expectation of privacy in his movements," which he "voluntarily conveyed to anyone who wanted to look."[98] In *United States v. Karo*, the Court held that the warrantless use of a beeper to track a subject in a private residence violated the Fourth Amendment; once a subject enters his home, he is no longer conveying his movements to the public.[99] Finally, in *Kyllo v. United States*, the Court found that the agents' failure to procure a warrant before using a thermal imaging device to "explore details of the home that would previously have been unknowable without physical intrusion" rendered it an unlawful search.[100]

Pursuant to *Katz*, *Knotts*, *Karo* and *Kyllo*, a Fourth Amendment analysis should focus on the public versus private aspects of information. Property "withdrawn from public view" should be entitled to Fourth Amendment protection (*Karo*).[101] A user's decision to privatize information suggests that the information should be treated as

telephone booth), but to a communication (the telephone conversation). Katz had a reasonable expectation of privacy neither because of who he was nor because of where he was, but because of what he was doing." Sklansky, *supra* note 30, at 195.

[98] *Knotts*, 460 U.S. at 281–82 (1983). In *Knotts*, the Court held that because the beeper was only used by law enforcement when the defendant was in public and thus in a place where he had no reasonable expectation of privacy, its use was lawful. *Id.* at 281.

[99] United States v. Karo, 468 U.S. 705, 715 (1984). In *Karo*, the Court found that "the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified." *Id.* Unlike the situation in *Knotts*, the defendant in *Karo* was not voluntarily conveying any information to the public. *Id*.

[100] Kyllo v. United States, 533 U.S. 27, 28, 40 (2001). The government's use of "sense-enhancing technology" to obtain information about the inside of the home that could not have been obtained without physical intrusion and a warrant constitutes a search because the "technology in question is not in general public use." *Id.* at 34.

[101] *Karo*, 468 U.S. at 716 ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.").

Bruce Van Baren argues that courts should apply the *Katz* test within the *Knotts* and *Karo* public/private framework. Under the public/private framework, "the Supreme Court should rule that the warrantless use of a GPS tracking device to track a suspect's movements outside his home does not constitute a 'search' or 'seizure' within the meaning of the Fourth Amendment." Bruce Van Baren, The Fourth Amendment in an Age of New Technologies: Circuits Split Over Warrantless GPS Tracking (Nov. 18, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1775402. *But see* United States v. Jones, 132 S. Ct. 945 (2012).

wholly private (*Kyllo*).[102] Private information in the cloud should not be considered within the sphere of "general public use"[103] even though a small number of people with particular computer expertise—the equivalent of "sense-enhancing technology" under *Kyllo*—can bypass encryption and password security inaccessible to the general public.[104] A policy that states that private information loses constitutional protection because expert computer hackers can access sensitive personal information would limit Fourth Amendment rights in the same way as the third-party doctrine.

This precedent makes clear that information stored in a private place and not conveyed to the public should be entitled to protection under the Fourth Amendment.

B. Content-Based Data

Government interception of the contents of communications analogous to cloud information constitutes a search and seizure under the Fourth Amendment.[105]

---

[102] *See Kyllo*, 533 U.S. at 33–34, 40.

[103] *See id.* at 34. David A. Sklansky states, "several lower courts [since Kyllo] (although certainly not all) have found the Fourth Amendment triggered by the use of binoculars or telescopes to spy on suspects in their own homes," even though binoculars and telescopes are certainly in "general public use." Sklansky, *supra* note 30, at 204–05 (2002). Sklansky believes that technology in "general public use," left constitutionally unregulated, could pose significant risks to Fourth Amendment protections. *Id.* at 204.

"In the long term, sensible interpretation of the Fourth Amendment will require the Court to acknowledge the differences between government surveillance and private snooping, and to abandon the assumption that anything knowingly exposed 'to the public' is therefore fair game for the police." *Id.* at 210.

Users may not mind if an ISP releases their personal information to advertisers. But they may have a problem if an ISP discloses that same information to the government. The third-party doctrine's applicability in the case of governmental disclosures is on completely different footing due to the possibility of criminal charges being filed.

[104] *Kyllo*, 533 U.S. at 34; *see also* Sklansky, *supra* note 30, at 201 ("Kyllo leaves unclear how 'general' public use of a monitoring technique must be before its use by the government will escape Fourth Amendment regulation, or even whether 'general public use' on any scale will have this effect. It therefore leaves open the possibility that continued, widespread hacking—or simply widespread use of programs that can be employed for hacking—will render even internet use from the home or office unprotected by the Fourth Amendment, as long as the government is content to use the same sorts of tools that hackers use.").

[105] *See* Smith v. Maryland, 442 U.S. 735, 741, 746 (1979) (finding no Fourth Amendment protection for the *numbers* dialed on a telephone); Smith v. State, 389 A.2d 858, 864 (Md. 1978) *aff'd*, 442 U.S. 735 (1979) ("It is generally held that the

The District Court for the Eastern District of New York found an exception to the third-party doctrine when government electronic surveillance intercepts the contents of communications. The court relied upon *Smith*, in which a pen register was distinguished from the bugging device in *Katz* on the basis that pen registers do not intercept the contents of communications.[106] The reasoning in *Smith* "implies that if pen registers recorded the contents of the communication . . . then a reasonable expectation of privacy may be preserved regardless of the communication's disclosure to the third-party phone company."[107]

In Missouri, an individual has a reasonable expectation of privacy in his text messages, as "subscribers assume that the contents of their text messages will remain private despite the necessity of a third party to complete the correspondence."[108] Although this assumption of

expectation of privacy protected by the [F]ourth [A]mendment attaches to the content of a telephone conversation."); Hadley v. State, 735 S.W.2d 522, 530 (Tex. App. 1987) (finding that the Fourth Amendment protects the contents of telephone conversations); United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (citing Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121 (2008)) (noting that the contents of emails are no less entitled to Fourth Amendment protection than the contents of mail); *see also* Kerr, *supra* note 66, at 1038 (2010); Slobogin, *supra* note 84, at 2.

Prior to government inspection of content-based data, probable cause and a warrant should be demonstrated. Warrants, however, are granted almost all of the time and may be bad for civil liberties. William J. Stuntz argued that warrantless searches are more regulated than searches with warrants—and he may have been right. "[A]nyone who works for the court system but who is not affiliated with the police department or prosecutor's office can be a magistrate." William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881, 889–89 (1991) ("The absence of any representative of the defendant surely biases warrant review in the government's favor. And the casual, quick review that the magistrate gives to most warrant applications is hardly as conducive to accurate application of the governing standard as the far more careful development of a record that characterizes suppression hearings.") (citing Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972)).

He continued, "if magistrates do a poor job of deciding whether probable cause exists, it is unclear why anyone should want them to do so more often, or indeed at all." *Id.* at 883.

[106] *In re* U.S. Application for an Order Authorizing the Release of Historical Cell Site Info., 809 F. Supp. 2d 113, 123 (E.D.N.Y. 2011) ("The content exception preserves the reasonable expectation of privacy, and thus Fourth Amendment protection, for some information to which strict application of the *Katz* test and the third-party-disclosure doctrine would not permit.").

[107] *Id.*

[108] State v. Clampitt, 364 S.W.3d 605, 611 (Mo. Ct. App. 2012).

privacy may not be reasonable in the post-Snowden era, cultural norms are such that we expect our personal data to remain private. This is especially true with material such as emails, texts and documents that would have been private in another format.

Orin Kerr suggests the adoption of a policy of technology neutrality, which "assumes that the degree of privacy the Fourth Amendment extends to the Internet should try to match the degree of privacy protection that the Fourth Amendment provides in the physical world."[109] "The deep roots of the content/non-content distinction in cases applying the Fourth Amendment to earlier communication networks suggests that it should not be out of place in the setting of the Internet."[110] Applying technology neutrality to cloud computing would mean that government acquisition of electronically-stored data would need to replicate government acquisition of data in its physical form.

C. Sensitive and Intimate Details

The government can attain a wealth of intimate details about an individual or business from search histories, data and emails. Without Fourth Amendment protections, law enforcement has unparalleled access to Americans' personal lives and work. When the information sought is sensitive, there is a greater intrusion into an individual's personal affairs, and the government's actions should constitute a search in violation of the Fourth Amendment.[111]

---

[109] Kerr, *supra* note 66, at 1038; *see also* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 577 (2009) ("The third-party doctrine responds with a rule that ensures roughly the same degree of privacy protection regardless of whether a criminal commits crimes on his own or uses third parties. The part of the crime that previously was open to observation—the transaction itself—remains open to observation. The part of the crime that previously was hidden—what the suspect did without third parties in his home—remains hidden. The result leaves the Fourth Amendment rule neutral as to the means of committing the crime: Using a third party does not change the overall level of Fourth Amendment protection over the crime.").

[110] *Id.*; *see also* Couillard, *supra* note 39, at 2231–32 ("[F]iles stored online are not transactional because their contents are not intended or required to be viewed by a third party, and [courts should] create a practical exception for certain quasi-transactional data such as URLs and passwords in order to respect the legitimate safeguards of virtual content.").

[111] *See* Dep't of Air Force v. Rose, 425 U.S. 352, 372–73 (1976) (finding, in interpreting a statute regarding a public disclosure of military records that contained an exemption for certain personnel records, that "Congress sought to construct an exemption that would require a balancing of the individual's right of privacy against the preservation of the basic purpose of the Freedom of Information Act . . . The device

"In determining whether a certain interest is a private affair . . . a central consideration is the nature of the information sought—that is, whether the information obtained" reveals intimate details of an individual's life.[112] Because of modern technological advancements, computers can "accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80."[113]

D. Shared Data

Government inspection of data, shared only among a limited group of people with user names and passwords, constitutes a search. The factors proposed above governing private data can apply to shared data. Confidential documents are drafted and shared on a daily basis with the expectation that they will not be shared outside the invited group of users.[114] For example, when several law firm associates simultaneously work on an appellate brief and the brief is stored on the firm's hard drive or left on a private desk when one of the associates leaves for home, a government inspection of the brief constitutes a

adopted to achieve that balance was the limited exemption, where privacy was threatened, for 'clearly unwarranted' invasions of personal privacy.").

[112] State v. Jordan, 156 P.3d 893, 896 (Wash. 2007).

[113] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 771 (1989). The Court further noted that, although "much rap-sheet information is a matter of public record, the availability and dissemination of the actual rap sheet [as a whole] to the public is limited." *Id.* at 753. Justice Sotomayor, in her concurring opinion in *Jones*, stated: "The Government can store such records and efficiently mine them for information years into the future." United States v. Jones, 132 S. Ct. 945, 955–56 (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting)).

[114] In the case of shared data, the government's engagement in electronic surveillance should not have a "chilling effect on people speaking their minds and expressing their views on important matters." United States v. White, 401 U.S. 745, 765 (1971) (Douglas, J., dissenting).

"Awareness that the Government may be watching chills associational and expressive freedoms." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (citing United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

A District Court of Appeal in Florida interpreted the freedom of association to include electronic communications. Enoch v. Florida, 95 So. 3d 344, 364 (Fla. Dist. Ct. App. 2012) ("The sweeping language in the 'electronic communication' provision [of a Florida anti-gang law] covers both criminal and innocent activity and, in doing so, prohibits expression and associational activity."); *see also* People v. Weaver, 12 N.Y.3d 433, 446 (N.Y. 2009) ("[M]eans of surveillance allowed the government to access an enormous amount of additional information, including a person's associations and activities.").

search. However, if the same lawyers collaborate electronically, they are left vulnerable to government search.

E. Intrusiveness

When determining whether an unconstitutional seizure has occurred the Supreme Court has also considered the intrusiveness of the government's methods in obtaining the information.[115] At "'the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[116]

There are degrees of intrusiveness. The examination of personal data in ISP storage is more intrusive than the observation of the same information stored on a public social media site.[117] Overly intrusive conduct in an electronic setting occurs when an individual has exhibited an expectation of privacy, the government examines his work (watching literally alongside him or watching his behavior clandestinely over the Internet), and the government search is overbroad.

Intrusions into the cloud to observe data stored on an ISP network should be justified only if the government's need for the information outweighs the government's degree of intrusiveness into an individual's constitutionally protected space. A court "must decide whether the practice . . . will significantly impair 'the people's' freedom from scrutiny."[118]

Computer cases frequently involve significant government intrusion—users store a tremendous amount of private information that can come into plain view, even in a targeted search.[119] The more

[115] A court looks at whether the government engages in "a particularly intrusive method of viewing." State v. Jackson, 76 P.3d 217, 222 (Wash. 2003) (quoting State v. Young, 867 P.2d 593, 598 (Wash. 1994)); *accord* Weaver, 12 N.Y.3d at 446; State v. Holden, 54 A.3d 1123, 1130 (Del. Super. Ct. 2010).

[116] Kyllo v. United States, 533 U.S. 27, 31 (2001) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

[117] *Compare* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (finding that individuals have a reasonable expectation of privacy in emails "stored with, or sent or received through, a commercial ISP") (internal citation omitted) *with In re* Application of United States for an Order Pursuant to 18 U.S.C. § 2703, 830 F. Supp. 2d 114, 133 (E.D.Va. 2011) (finding that Twitter users had no expectation of privacy in their IP information because they voluntarily disclosed it to Twitter as a condition of use).

[118] State v. Campbell, 759 P.2d 1040, 1047–49 (Or. 1988).

[119] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005). Kerr states that courts must take care to limit the scope of warrants. *Id.* at 536.

intrusive the method, the greater a citizen's constitutional protection should be.[120]

It is the role of the Court to ensure the protections of the Fourth Amendment. Especially when Congress does not act, the Court has the difficult responsibility of distinguishing between legally executed techniques and their aggregation into overly invasive behemoths of executive action voiding the privacy protections explicitly embedded in our Constitution. The Court should use the factors outlined in this article to ensure the appropriate balance between security and liberty. Inspection of data stored in the cloud should be presumed to be a search; however, the government should be able to rebut this in certain circumstances.

Riley set forth a similar balancing test to determine whether a warrantless search of digital data would create an unconstitutional invasion of privacy. This test requires analysis of the "degree to which [the search] intrudes upon an individual's privacy" versus "the degree to which [the search] is needed for the promotion of legitimate governmental interest."[121] *Riley* has reinforced the notion that the benefits to society must be greater than the invasion into an individual's private matters in order for a warrantless search of digital data to be constitutional. An almost identical test should be applied to digital data stored on the cloud.

IV. STATUTORY PROTECTION

"*Hey, hey, you, you, get off of my cloud.*"[122]

Edward Snowden's disclosure of the highly secretive PRISM program illustrated that the government has the means to monitor our

Technological searches "may allow warrants that are particular on their face to become general warrants in practice." *Id.* "The dynamics of computer searches upset the basic assumptions underlying the plain view doctrine. More and more evidence comes into plain view, and the particularity requirement no longer functions effectively as a check on dragnet searches." *Id.* at 576–77.

[120] The Indiana case of *State v. Thomas* provides an example of an overly intrusive method: "Video surveillance is highly intrusive and amenable to abuse, and a *warrantless* video search poses a serious threat to privacy." State v. Thomas, 642 N.E.2d 240, 247 (Ind. Ct. App. 1994).

[121] Riley v. California, 134 S. Ct. 2473, 2484 (2014) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[122] THE ROLLING STONES, *Get Off of My Cloud*, *on* DECEMBER'S CHILDREN (AND EVERYBODY'S) (London Records 1965).

online activities and that ISPs routinely hand citizens' data over to the government without a court order.[123] Two statutes regulate electronic communications, the Stored Communications Act (SCA) and Foreign Intelligence Surveillance Act (FISA).[124]

A. The Inadequacy of the Stored Communications Act

In addition to the Fourth Amendment, the SCA, enacted by Congress before the proliferation of the Internet, may protect cloud data. Unfortunately, the SCA is insufficient and obsolete and must be updated to deal with modern challenges like cloud-based computing.[125]

There are significant problems with the SCA that render it unworkable in the context of data stored in the cloud. First, its definitions do not apply to modern technology. Second, the SCA applies only to "providers to the public" such as Apple and Google. Third, and most worrisome, the act fails to provide suitable protection for the contents of information stored in the cloud.

The level of privacy protection afforded by the act depends on whether an entity provides an electronic communication service (ECS) or a remote computing service (RCS). An ECS provider is defined in the Act as an entity that provides users with "the ability to send or receive wire or electronic communications."[126] Section 2510 of the United

[123] The Guardian reported that some major technology companies have taken steps to make it easier for intelligence agencies to access information. Dominic Rushe, *Technology Giants Struggle to Maintain Credibility Over NSA PRISM Surveillance*, THE GUARDIAN (June 9, 2013, 3:37 PM), http://www.theguardian.com/world/2013/jun/09/technology-giants-nsa-prism-surveillance. Yahoo, Microsoft, Google, Facebook and Apple are involved with the PRISM program. *Id.* "Companies are required to comply with directives for information, but there is evidence that some have been able to delay or resist." *Id.* "Twitter was a notable exception to the list and has reportedly declined to co-operate. Amazon, which offers back office services to a huge number of web companies, is also missing." *Id.* But this degree of cooperation may be changing. *See* David E. Sanger & Matt Apuzzo, *F.B.I. Director Hints at Action as Google and Apple Lock Up Cellphone Data*, N.Y. TIMES, Oct. 17, 2014, at A19, *available at* http://www.nytimes.com/2014/10/17/us/politics/fbi-director-in-policy-speech-calls-dark-devices-hindrance-to-crime-solving.html.

[124] *See generally* 18 U.S.C. § 2701 (2009); 50 U.S.C. § 1801 (2010). ISP user agreements are drafted to comply with the SCA and the FISA; they notify users that their material can be transferred to the government upon request and without notice.

[125] For a thorough discussion of the SCA, see Mulligan, *supra* note 68.

[126] 18 U.S.C. § 2510(15) (2002). "Electronic Storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic

States Code was intended to apply to "large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing."[127] The government is required to obtain a warrant supported by probable cause before it can gain access to content stored in an ECS for 180 days or less.[128] If content has been stored for more than 180 days, the government must (1) obtain a search warrant without notice to the subscriber; (2) present a provider with an administrative or grand jury subpoena with notice to the subscriber; or (3) obtain a court order for disclosure with notice to the subscriber.[129]

On the other hand, a RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[130] To gain access to data stored by

transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(A)-(B) (West 2002).

[127] S. REP. NO. 541 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555.

[128] 18 U.S.C. § 2703(a) (2009).

[129] 18 U.S.C. § 2703(a)-(b), (d) (2009). If the government obtains the information through a subpoena or court order, some circumstances may permit delayed notice to the subscriber for up to 90 days, with the possibility for extensions of time. 18 U.S.C. § 2703(b)(B) (2009) ("[D]elayed notice may be given pursuant to section 2705 of this title."); 18 U.S.C. § 2705(a) (2009) (stating that a court shall grant an order delaying notice to the subscriber if "there is reason to believe that notification of existence of the court order [or subpoena] may have an adverse result," including "endangering the life or physical safety of an individual," "flight from prosecution," "destruction of or tampering of evidence," "intimidation of potential witnesses," or "otherwise seriously jeopardizing an investigation or unduly delaying a trial."). The government may apply for a court order pursuant to 18 U.S.C. § 2705(a) "commanding a provider of [ECS] or [RCS] to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." 18 U.S.C. § 2705(b) (2009). The reasons justifying such an order are the same as those that justify delayed notice (enumerated in 18 U.S.C. § 2705(a)(2)). 18 U.S.C. § 2705(b) (2009).

[130] 18 U.S.C. § 2711(2) (West 2009). Legislative history indicates that the RCS category was included in the SCA in response to the volume of businesses using third-party off-site remote storage systems. S. REP. NO. 99-541, at 3, *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557, 3564–65 ("In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data in-house on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing.").

an RCS provider, the government can (1) obtain a search warrant without notice to the subscriber, (2) present a provider with an administrative or grand jury subpoena with notice to the subscriber, or (3) obtain a court order for disclosure with notice to the subscriber.[131] If the government obtains the information through a subpoena or court order, some circumstances may permit delayed notice to the subscriber for up to 90 days, with the possibility for extensions of time.[132]

Some types of cloud computing may fit within the definition of an RCS, although it is difficult to know since cloud computing was not in existence at the time the SCA was enacted. If a provider offers its services to the public (many do not), and if it provides storage or processing services by means of an electronic communications system (as compared to storage or processing not intended as a communication), then the minimal protection offered by the SCA could be available. Because the ECS category applies to ISPs that provide users with the ability to send or receive information, cloud storage may not fall within this category because it is not a communication. However, email stored in the cloud may fall into the ECS category if the primary purpose of the ISP is to provide users with the ability to send and receive electronic communications.

The government can acquire content data that has been stored by a public ISP for more than 180 days with nothing more than an administrative subpoena if it demonstrates "specific and articulable facts"—not probable cause—that the records are relevant and material to an ongoing criminal investigation.[133] Some lower courts have held that the SCA's "specific and articulable facts" standard, a lower standard

---

[131] 18 U.S.C. § 2703(a)-(b) (2009).

[132] 18 U.S.C. § 2703(b)(B) (2009) ("[D]elayed notice may be given pursuant to section 2705 of this title."); 18 U.S.C. § 2705(a) (2009) (stating that a court shall grant an order delaying notice to the subscriber if "there is reason to believe that notification of existence of the court order [or subpoena] may have an adverse result," including "endangering the life or physical safety of an individual," "flight from prosecution," "destruction of or tampering of evidence," "intimidation of potential witnesses," or "otherwise seriously jeopardizing an investigation or unduly delaying a trial.").

Pursuant to 18 U.S.C. § 2705(a), the government can apply for a court order "commanding a provider of [ECS] or [RCS] to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." 18 U.S.C. § 2705(b) (2009). The reasons justifying such an order are the same as those that justify delayed notice (enumerated in 18 U.S.C. § 2705(a)(2)). 18 U.S.C. § 2705(b) (2009).

[133] 18 U.S.C § 2703(c)(1), (d) (2012).

than probable cause, violates the Fourth Amendment,[134] while others have held the provision constitutional.[135] The Sixth Circuit has found this provision of the SCA allowing the government to obtain content-based data without warrant and judicial oversight to be unconstitutional.[136] The court concluded that there is a reasonable

[134] *In re* Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578 (E.D.N.Y. 2010), *rev'd*, No. 10–MC–0550 (E.D.N.Y. Nov. 29, 2011) (unpublished order noting written opinion to follow) (finding that the government must obtain a warrant before requiring a cell phone provider to disclose a subscriber's historical cell site information and an order issued under the "specific and articulable facts" standard violated the Fourth Amendment); *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., No. 11–MC–0113 (JO), 2011 WL 679925, at *1 (E.D.N.Y. Feb. 16, 2011) (finding that an order under the SCA that institutes long-term tracking via cell-site information requires a warrant, but shorter-term tracking is constitutional under the "specific and articulable facts" standard); *In re* Application of United States for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674, 675, 676–78 (S.D. Tex. 2013) (finding that cell tower dumps, which contained large amounts of cell phone data from five different providers, were not addressed by the SCA, cannot be obtained pursuant to the "specific and articulable facts" standard of §2703(d), and require a warrant supported by an affidavit showing probable cause).

[135] *In re* Application of United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *10-12 (D. Ariz. May 8, 2013) (finding that the government's acquisition of cell-site records does not constitute a search under the Fourth Amendment and such records can constitutionally be obtained through the SCA under the "specific and articulable facts" standard); United States v. Gomez, No. 10–321, 2012 WL 3844370, at *2 (E.D. Pa. Sept. 5, 2012) (finding that warrantless installation of a GPS device on defendant's vehicle and subsequent tracking of the vehicle did not violate the Fourth Amendment); United States v. Madison, No. 11–60285–CR, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012) ("[T]he Fourth Amendment does not impose a probable-cause requirement on the obtaining of cell-tower information," and the government need only meet the standard set forth in the SCA.) (quoting 18 U.S.C. § 2703(d)); United States v. Dye, No. 1:10CR221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011) (finding no reasonable expectation of privacy in cell phone records or cell site location information); United States v. Velasquez, No. CR 08–0730 WHA, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010) (finding no reasonable expectation of privacy in cell site location information); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010) (finding no legitimate expectation of privacy in cell phone records); United States v. Suarez–Blanca, No. 1:07–CR–0023–MHS/AJB, 2008 WL 4200156, at *8–11 (N.D. Ga. Apr. 21, 2008) (finding that the government's acquisition of cell site information did not violate the Fourth Amendment because the data only showed historical location information and the records maintained by the cell phone company qualified as business records).

[136] United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without

expectation of privacy in this information because "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[137]

Similarly, the District Court for the Eastern District of New York found that the SCA's "specific and articulable facts" standard permits the Government to "map our lives."[138] In order to obtain content-based records in New York, the court held, the government must demonstrate probable cause.[139]

The Third Circuit found that a standard lesser than "probable cause" and greater than "specific and articulable facts" is more likely the appropriate standard with regard to cell site information.[140] The court

first obtaining a warrant based on probable cause . . . Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.").

Orin S. Kerr states that this provision of the SCA is unconstitutional because it "permits the government to obtain the contents of some remotely stored Internet files with less process than a warrant . . . It also allows a provider to disclose the contents of an account used for remote storage, such as those popular with cloud computing, without a warrant." Kerr, *supra* note 66, at 1043 (2010).

[137] *Warshak*, 631 F.3d at 286.

[138] *In re* U.S. Application for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 114–15 (E.D.N.Y. 2011). The court stated, in SCA cases, in addition to finding "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication or other records, are relevant and material to the ongoing criminal investigation," a court must also "consider whether granting the order requested would violate the Fourth Amendment." *See id.* SCA's "specific and articulable facts" standard does not pass muster under the Fourth Amendment. *See id.* Before a government entity can obtain the records of a cellular telephone company or ISP, an order must be obtained requiring a showing of probable cause. *See id.* Cumulative cell-site location records constitute an exception to the third-party disclosure doctrine. *See id.*

[139] *Id.*

[140] *In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 307 (3d Cir. 2010). The court found that the SCA gives a magistrate judge the discretion to require a warrant, issued upon a showing of probable cause, in addition to the court order sought under § 2703(d) but such option should be "used sparingly because Congress also included the option of a § 2703(d) order." *Id.* at 319. Cell site location information that allows the government to track individuals via their cell phones is "information from a tracking device deriving from an electronic communications service" and the government cannot obtain such information under 18 U.S.C. § 2703(d) and must, instead, obtain a warrant. *Id.* at 309. The court found that, "[a]lthough the language of § 2703(d) creates a higher standard than that required by the pen register and trap and

held that the SCA grants a judge the option of requiring a warrant and does not require the issuance of an order based solely upon a showing of "specific and articulable facts."

The Eleventh Circuit has also weighed in. In *United States v. Davis,* the court found that *United States v. Jones* was instructive in deciding whether historical cell site information stored by a service provider was protected under the Fourth Amendment.[141] Finding "that the privacy theory is not only alive and well, but available to govern electronic information of search and seizure in the absence of trespass,"[142] the court held that the government's "warrantless gathering" of the defendant's cell site location information violated his reasonable expectation of privacy.[143] Turning to the applicability of the third-party doctrine due to the involvement of the cellular provider, the Eleventh Circuit referred to the Third Circuit's approach.[144] Using this approach, the court held that the defendant did "not voluntarily disclose[] his cell site location information to the provider in such a fashion as to lose his reasonable expectation of privacy."[145]

In contrast, the United States Court of Appeals for the Fifth Circuit held that probable cause is not required by the SCA in order for the government to be granted access to historical cell site data.[146] The court found that the SCA conforms to existing precedent which "does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure."[147] Accordingly, the court declined "to create a new rule to hold that Congress's balancing of privacy and safety is unconstitutional."[148]

With five different circuits applying different approaches, it is

trace statutes, the legislative history provides ample support for the proposition that the standard is an intermediate one that is less stringent than probable cause." *Id.* at 305.

[141] United States v. Davis, 754 F.3d 1205, 1213 (11th Cir. 2014) *reh'g en banc granted and opinion vacated*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014).

[142] *Id.* at 1215.

[143] *Id.*

[144] *In re* Application of United States for an Order Directing a Provider of Elec. Commnc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

[145] *Id.* at 1217.

[146] United States v. Guerrero, 768 F.3d 351 (5th Cir. 2014); *In re* Application of United States for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013).

[147] *In re Application of United States for Historical Cell Site Data*, 724 F.3d at 615.

[148] *Id.*

apparent that the SCA is no longer workable. For example, if an ISP, like Google, provides both ECS and RCS, it would be within a court's discretion whether to apply ECS or RCS provisions. If RCS provisions were applied, the government could obtain the contents of all emails and documents with a subpoena, without any demonstration of cause or notice to the subscriber, at any time. If ECS provisions were applied, the government would need a warrant supported by probable cause during the first 180 days, but after six months could obtain the contents of emails and documents with a subpoena and without any showing of cause or notice to the subscriber. The difference between the two provisions is in fact the length of time the government has to wait to secure the data.

In addition, the SCA only applies to "providers to the public" such as Apple and Google. Private ISPs not available to the "community at large," which organizations hire to store and secure their data, are not protected by the Act at all.[149]

In sum, the SCA authorizes the government to take non-private information without a warrant or user notice. While legislation could remedy the problems presented by the SCA, all Congressional efforts to enact new law to balance Internet privacy with government access have failed.[150]

B. The Foreign Intelligence Surveillance Act and United States Citizens

In FISA, Congress authorized the government to conduct searches pursuant to statutes designed and enacted to prevent terrorism. FISA is considered exempt from the probable cause requirement because it is aimed at preventing terrorism, not just ordinary criminal

[149] Another problem with the SCA is that it prohibits private causes of action against ISPs that disclose information to the government pursuant to this section. 18 U.S.C. § 2703(e).

[150] Gerry Smith, *Senate Won't Vote on CISPA, Deals Blow to Controversial Cyber Bill*, HUFFINGTON POST (Apr. 25, 2013, 7:13 PM), http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html; *see* Brian Fung, *Why Waiting for Congress to Fix Cybersecurity is a Waste of Time*, WASH. POST (Aug. 1, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/01/why-waiting-for-congress-to-fix-cybersecurity-is-a-waste-of-time ("There are things that only an act of Congress can accomplish, of course. But given the progression of proposals we've seen over time, placing expectations in the hands of bureaucrats rather than lawmakers might be a safer bet.").

wrongdoing. Although the FAA provides that any "surveillance must comply with the Fourth Amendment," the Amendment's reasonableness requirement is not satisfied by either the FAA or the original FISA statute.[151] This is because: (1) FISA lacks a probable cause requirement; (2) FISA does not require the government to release the fruit of the government's investigation; and (3) FISA is not limited to investigations involving international terrorism.[152]

When Americans are prosecuted based upon evidence

[151] 50 U.S.C. § 1804(a)(5) (2010) (governing surveillance conducted pursuant to a court order under FISA as originally enacted); 50 U.S.C. § 1881a(b)(5) (2008) (governing surveillance authorized by the Attorney General and the Director of National Intelligence pursuant to the 2008 FISA amendments). *See* 50 U.S.C. § 1804(a)(5) (2010); 50 U.S.C. § 1881a(b)(5) (2008).

[152] Pursuant to 50 U.S.C. § 1805(a)(2) (2010), a court shall issue an order authorizing surveillance if "probable cause" is shown that the target is a foreign power and the locations where surveillance is directed are being used by the foreign power. 50 U.S.C. § 1805(a)(2) (2010).

However, this "probable cause" is not the same as the probable cause requirement of the Fourth Amendment. Black's Law Dictionary defines "probable cause" in the criminal context as "[a] reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items connected with a crime." BLACK'S LAW DICTIONARY (9th ed. 2009). Neither Section 1805 nor Section 1881a requires a showing of probable cause that a crime has been committed or is being committed. *See also* Owen Fiss, *Even in a Time of Terror*, 31 YALE L. & POL'Y REV. 1, 20 (2012). The 2008 FISA amendments never "require the suspicion of criminality that is the essence of probable cause." *Id.* at 21.

The 2008 amendments further expanded governmental authority, diminished Fourth Amendment protections for United States citizens and "severed the analytic connection between international terrorism and wiretapping and justified such surveillance as a form of intelligence gathering, which included, but was not limited to, the surveillance of persons suspected of international terrorism directed against the United States." *Id.* at 3.

Another problem with the FISC is the absence of defense counsel. A privacy advocate with the responsibility of representing the defense perspective should be present in court during FISC proceedings. A privacy advocate would be subject to the same confidentiality as others working in the court, and would be required to maintain the secrecy necessary to the FISC. Retired federal judge James Robertson, who served on the FISC from 2002 to 2005, told an oversight panel in July 2013 that judges need to hear both sides of a case before deciding and that "[t]his process needs an adversary." Doyle McManus, *Hire a Devil's Advocate: Our Secret Surveillance Court Shouldn't Hear Only One Side*, PITTSBURGH POST-GAZETTE (July 29, 2013, 12:00 AM), http://www.post-gazette.com/stories/opinion/perspectives/hire-a-devils-advocate-our-secret-surveillance-court-shouldnt-hear-only-one-side-697260. Jeffrey Smith, a former general counsel at the CIA, stated, "I think it should be a lawyer in the executive branch." *Id.*

discovered during surveillance of a foreign target, this use presents Constitutional concerns.[153] FISA authorizes the Foreign Intelligence Surveillance Court (FISC) to issue orders requiring commercial ISPs to disclose private user information to the government without notice to targets.[154] In addition, language in the FISA Amendments Act of 2008 (FAA) permits the government, under exigent circumstances, to conduct surveillance that may involve United States citizens, without first obtaining the approval of the FISC.[155] Pursuant to the FAA, the NSA is

[153] United States citizens cannot be the targets of FISA surveillance. 50 U.S.C. § 1802(a)(1)(A)-(B) (2010) (providing that the President may not authorize electronic surveillance without a court order unless the surveillance is directed solely at acquiring "communications used exclusively between or among foreign powers" and "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party"); 50 U.S.C. § 1804(a) (2010) (providing that an application for a court order for electronic surveillance must include a statement of facts by the applicant to justify his belief that the target of surveillance is a foreign power and the facilities or places where the surveillance will be conducted are being used or are about to be used by a foreign power). Any information concerning a United States person that is obtained via surveillance conducted pursuant to this chapter "may be used and disclosed . . . without the consent of the United States person only in accordance with the minimization procedures." 50 U.S.C. § 1806(a) (2008). Any disclosure of such information must be "accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General." 50 U.S.C. § 1806(b) (2008).

Neither United States citizens nor foreigners are prosecuted in the FISC. The FISC's only purpose is to "hear applications for and grant orders approving electronic surveillance anywhere in the United States" pursuant to FISA. 50 U.S.C. § 1803(a) (2010).

[154] 50 U.S.C. § 1805(c)(2) (2010). No information obtained via surveillance under this chapter may be disclosed for law enforcement purposes unless such "information, or any information derived therefrom," is to be used in a criminal proceeding. 50 U.S.C. § 1806(b) (2008).

[155] Pursuant to 50 U.S.C. § 1881a, the Attorney General and the Director of National Intelligence may jointly authorize surveillance of people outside the United States for a period of up to one year for the purpose of acquiring foreign intelligence information. The surveillance may be conducted pursuant to Section 1881a if either: (1) the Attorney General and Director of National Intelligence determine "that exigent circumstances exist" or (2) the FISC issues an order under 50 U.S.C. § 1881a(i)(3). 50 U.S.C. § 1881a (2008).

50 U.S.C. § 1881a(b) (2008) outlines the limitations of such surveillance, including that the surveillance may not target anyone known to be in the United States, anyone outside the United States if the purpose is to target a person inside the United States, or a United States person who is outside the United States. In addition, the surveillance must comply with the Fourth Amendment. 50 U.S.C. § 1881a(b)(5) (2008).

systemically conducting warrantless searches of the contents of Americans' email and text communications, hunting for people who mention information about foreigners who are targets of FISA surveillance.[156]

This surveillance results in the prosecution of American citizens who were not targets of the surveillance. For example, if a foreign target of investigation communicates via email with a United States citizen, the government, in a criminal prosecution of this American citizen, can introduce any of his statements that were discovered during surveillance of the foreign target.[157] The government need only provide reasons for believing a target is a foreign power or agent thereof and that a "significant purpose of the surveillance is to obtain foreign intelligence information."[158] Thus, under FISA, incidental third parties can be

At a House Intelligence Committee oversight hearing in June 2013, the deputy director of the NSA, John Inglis, stated, "We do not target the content of U.S. person communications without a specific warrant anywhere on the earth." Charlie Savage, Broader Sifting of Message Data by N.S.A. Is Seen, N.Y. Times, Aug. 8, 2013, at A1, available at http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html.

[156] Savage, *supra* note 155.

[157] 50 U.S.C. § 1801(i) (2010) (defining "United States person" as a "citizen of the United States," as well as an "alien lawfully admitted for permanent residence"); 50 U.S.C. § 1806 (West 2008) (outlining the permissible and lawful uses of information obtained by the government via FISA surveillance); *see also* Fiss, *supra* note 152, at 24 n.96 (citing United States v. Perillo, 333 F. Supp. 914, 919–21 (D. Del. 1971)); United States v. Kahn, 415 U.S. 143, 157 (1974) (holding that the government's interception of incriminating telephone calls by the wife of a target of surveillance, and the subsequent use of those calls in a criminal prosecution against the wife, did not violate the Fourth Amendment even though the government had not established probable cause regarding the wife before beginning surveillance).

[158] 50 U.S.C. § 1804(a)(6)(B) (2010). As originally enacted, FISA required that the acquisition of foreign intelligence information be "the purpose" for which a warrant was sought. United States v. Abu-Jihaad, 630 F.3d 102, 126 (2d Cir. 2010) (citing 50 U.S.C. § 1804(a)(7)(B) (Supp. V 1981)). However, following the 2001 FISA amendments, Congress indicated that the acquisition of foreign intelligence need not be the "primary purpose" of the surveillance, but only a "significant purpose" of the surveillance. *Abu-Jihaad*, 630 F.3d at 126; *see* 50 U.S.C. § 1805 (2010).

In order to issue an order authorizing the surveillance, the FISC need only find "probable cause" to believe that the target is a foreign power or agent thereof and that the places or facilities where the electronic surveillance will be directed are being used or are about to be used by the foreign power or agent thereof. 50 U.S.C. § 1805(a)(2) (2010). However, this requirement only applies to court-ordered FISA surveillance. Surveillance conducted pursuant to the FAA is subject to different requirements. *See* 50 U.S.C. § 1881a (2008).

participants in intercepted communications with targets being investigated, without probable cause, by the government.[159] This practice renders FISA unconstitutional as applied to United States citizens because it permits the government to investigate foreign targets without probable cause, even when Americans are incidental parties to the investigation.[160]

Even more worrisome, the government has refused to turn over the fruits of these FISA investigations, even after defendants are charged with crimes based upon evidence discovered during FISA surveillance.[161] The government claims that FISA simply requires it to notify defendants that they have acquired such information and does not require them to disclose the contents of such information.[162] This

See also Memorandum from John C. Yoo, Deputy Assistant Att'y Gen., to David S. Kris, Assoc. Deputy Att'y Gen., on the Constitutionality of the Amendment Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches (Sept. 25, 2001) [hereinafter Yoo Memorandum], *available at* 2001 WL 36191050, at *8. According to the Office of Legal Counsel (OLC), "while FISA states that 'the' purpose of a search is for foreign intelligence, that need not be the only purpose. Rather, law enforcement considerations can be taken into account, so long as the surveillance also has a legitimate foreign intelligence purpose." *Id.* The OLC noted that some courts require that the "primary purpose" of the FISA surveillance must be obtaining foreign intelligence, but not all courts have applied that test. *Id.* The OLC stated that, as long as "the government has a legitimate objective in obtaining foreign intelligence information, it should not matter whether it also has a collateral interest in obtaining information for a criminal prosecution." *Id.* at *9.

[159] 50 U.S.C. § 1881a (2008). Owen Fiss states that this grant of authority pursuant to the FAA "should be declared invalid under the doctrine that condemns overbroad interferences with freedom." Fiss, *supra* note 152, at 3.

[160] FISA, as originally enacted, contained a "probable cause" requirement, but it does not resemble the probable cause required by the Fourth Amendment. *See* 50 U.S.C. § 1805(a)(2) (2010); *see also* 50 U.S.C. § 1881a (2008) (authorizing the "targeting of persons reasonably believed to be located outside the United States").

[161] 50 U.S.C. 1806(c) (2008) applies to information acquired under FISA, pursuant to a court order, as well as information acquired under 1881a, without a court order. It states that if the government intends to use "information obtained or derived from an electronic surveillance of [an] aggrieved person" in a trial, hearing, or other proceeding, "the Government shall . . . notify the aggrieved person . . . that the Government intends to so disclose or so use such information." 50 U.S.C. § 1806(c) (2008); *see also* 50 U.S.C. § 1881e (2008) (providing that any information obtained pursuant to 50 U.S.C. § 1881a surveillance, which provides additional procedures for electronic surveillance of foreign targets, is subject to the same requirements as 50 U.S.C. § 1806).

[162] "[I]f the Government intends to use or disclose information obtained or derived from a §1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the

practice is being challenged in various cases around the country.[163]

V. THE SPECIAL NEEDS DOCTRINE AND NATIONAL SECURITY

Finally, the special needs doctrine is being used to justify the indiscriminate acquisition of personal data. Although diminished Fourth

acquisition." 50 U.S.C. §§1806(c), 1806(e), 1881e(a) (2006 & Supp. V); Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1154 (2013).

Solicitor General Verrilli stated to the Court during oral argument in *Clapper* that an aggrieved party whose communication is intercepted and against whom proceedings are initiated has a right to notice or disclosure of the information obtained via surveillance. Transcript of Oral Argument, Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013) (No. 11-1025), 2012 WL 5305254.

In the Clapper opinion, the Court noted:

> "[I]f the Government were to prosecute one of respondent-attorney's foreign clients using § 1881a-authorized surveillance, the Government would be required to make a disclosure. Although the foreign client might not have a viable Fourth Amendment claim, it is possible that the monitoring of the target's conversations with his or her attorney would provide grounds for a claim of standing on the part of the attorney."

Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1154 (2013) (internal citation omitted).

[163] New York Times Reporter Adam Liptak wrote that federal prosecutors have not disclosed FISA information:

> In a prosecution in Federal District Court in Fort Lauderdale, Fla., against two brothers accused of plotting to bomb targets in New York, the government has said it plans to use information gathered under the Foreign Intelligence Surveillance Act of 1978, or FISA, which authorized individual warrants. But prosecutors have refused to say whether the government obtained those individual warrants based on information derived from the 2008 law, which allows programmatic surveillance. Prosecutors in Chicago have taken the same approach in a prosecution of teenager accused of plotting to blow up a bar. In the Fort Lauderdale case, Magistrate Judge John J. O'Sullivan ordered the government to disclose whether it had gathered information for the case under the 2008 law. He relied on Justice Alito's statement in the Clapper decision. The government has moved for reconsideration. By insisting that they need not disclose whether there had been surveillance under the 2008 law, the two sets of prosecutors have so far accomplished precisely what Mr. Verrilli said would not happen. They have immunized the surveillance program from challenges under the Fourth Amendment, which bans unreasonable searches and seizure. Yet there is excellent reason to think that surveillance under the 2008 law, the FISA Amendments Act, was involved in both cases.

Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES, July 15, 2013, at A11, *available at* http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html; *see* United States v. Qazi, No. 12–60298–CR–Sco1a, 2012 WL 7050588 (S.D. Fla. Dec. 19, 2012); United States v. Kashmiri, No. 09 CR 830–8, 2012 WL 3779107 (N.D. Ill. Aug. 30, 2012).

Amendment standards are justifiable under certain well-defined emergencies, the circumstances must be reasonable, limited and previously delineated.[164] However, in the context of national security cases, application of FISA and the special needs doctrine should be limited to prosecutions involving terrorism.

When "special needs" beyond the normal need for law enforcement make the warrant requirement impractical, no warrant is required.[165] The reasoning is that minimal intrusion on privacy can be justified by the government's need to combat an overriding public danger.[166]

The Court has only applied the special needs doctrine in "certain limited circumstances" when "the Government's need to discover . . . latent or hidden conditions, or to prevent their development, is sufficiently compelling to justify the intrusion on privacy entailed by conducting such searches without any measure of individualized suspicion."[167]

The FISC, however, has expanded the use of the special needs doctrine in terrorism cases.[168] "That legal interpretation is significant . . .

---

[164] *See, e.g.*, Lebron v. Sec'y, Fla. Dep't of Children and Families, 710 F.3d 1202, 1206–07 (11th Cir. 2013).

[165] Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602 (1989); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989); City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

[166] *See, e.g.*, *Lebron* at 1207–08.

[167] *Von Raab*, 489 U.S. at 668.

[168] *See Skinner*, 489 U.S. at 619; Yoo Memorandum, *supra* note 158. The Office of Legal Counsel (OLC) addressed the constitutionality of authorizing a search pursuant to FISA if foreign intelligence gathering is "a purpose" of the search, as opposed to "the purpose" of the search. The OLC stated that the proposed amendments to FISA (later enacted as the FISA Amendments Act (FAA)) did not violate the Fourth Amendment because they simply allowed the government to "apply for FISA warrants up to the limit permitted by the Constitution." *Id.* The OLC stated, "the government could conduct searches to obtain foreign intelligence without satisfying all of the requirements applicable in the normal law enforcement context." *Id.* at *3.

The OLC justified this warrantless surveillance under the special needs doctrine, concluding that "the Fourth Amendment's reasonableness test for searches generally calls for a balancing of the government's interest against the individual's Fourth Amendment interests," and that in the case of obtaining counter-intelligence for the purpose of protecting national security, "the government interest is great." *Id.* Further, the OLC stated that "[t]he factors favoring warrantless searches for national security reasons may be even more compelling . . . After the attacks on September 11, 2001." *Id.* at *4.

because it uses a relatively narrow area of the law — used to justify airport screenings, for instance, or drunken-driving checkpoints — and applies it much more broadly, in secret, to the wholesale collection of communications in pursuit of terrorism suspects."[169] The special needs doctrine applies in these cases on the theory that if the government collects data from all of its citizens for the special need of national security, the Fourth Amendment is not violated.[170]

The application of the special needs doctrine to national security investigations is an impermissibly overbroad use of the doctrine. Supreme Court precedent makes clear that the government cannot use

The OLC stated, "the President's constitutional responsibility to defend the nation may justify reasonable, but warrantless, counter-intelligence searches." *Id.* at *7. Further, "the current situation, in which Congress has recognized the President['s] authority to use force in response to a direct attack on the American homeland, has changed the calculus of a reasonable search." *Id.* at *8. The OLC concluded, "like the warrant process in the normal criminal context, FISA represents a statutory procedure that, if used, will create a presumption that the surveillance is reasonable under the Fourth Amendment." *Id.*

But see Memorandum from Steven G. Bradbury, Principal Deputy Assistant Att'y Gen. on the Status of Certain OLC Opinions Issued in the Aftermath of the Terrorist Attacks of September 11, 2001(Jan. 15, 2009) (revising its September 25, 2001 opinion), *available at* 2009 WL 1267352, at *10. In its 2009 opinion, the OLC stated, "the Supreme Court has recognized warrantless searches to be 'reasonable' in a variety of situations involving 'special needs' that go beyond the routine interest in law enforcement." *Id.* The OLC emphasized that warrantless surveillance may be justified under the special needs doctrine. *Id.* However, to the extent that its September 25, 2001, opinion relied on "self-defense" cases as a justification for the government's warrantless surveillance as a way to protect the nation, it redacted its former opinion. *Id.* at *10. "The 9/25/01 FISA Opinion's assertion that '[i]f the government's heightened interest in self-defense justifies the use of deadly force, then it certainly would also justify warrantless searches' does not adequately account for the fact-dependent nature of the Fourth Amendment's 'reasonableness' review." *Id.*

[169] Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES, July 6, 2013, at A1, *available at* http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.

[170] *See, e.g.*, John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 HARV. J. L. & PUB. POL'Y 901, 920–23 (2014), *available at* http://scholarship.law.berkeley.edu/facpubs/2394. In the special needs case of *Skinner v. Ry. Labor Execs. Ass'n*, the Court allowed drug and alcohol testing of railway workers after their involvement in an accident. *Skinner*, 489 U.S. 602. The Court held that although the testing constituted a Fourth Amendment search, the government's need to ensure railroad safety justified the application of the "special needs" doctrine, eliminating the need for the government to require a warrant before testing. *Id.* at 617, 620.

evidence collected in a national security investigation for a subsequent unrelated criminal prosecution purpose.[171] For example, in *National Treasury Employees Union v. Von Raab*, the Court held that although employees who tested positive for drugs could be subject to dismissal, the test results could not be turned over to criminal prosecutors without the employee's written consent.[172]

Once the government seeks to use evidence acquired from a special needs search for another purpose, a new and completely different privacy issue analysis is necessary.[173] For example, in *Maryland v. King*, the Court held that DNA swabs of inmates could be used for identification purposes only.[174] If the DNA swabs were used for any other purpose, a completely different privacy issue arises.[175]

---

[171] In order for the special needs doctrine to apply, the primary purpose of the investigation must not be to detect ordinary criminal wrongdoing. City of Indianapolis v. Edmond, 531 U.S. 32, 41–42 (2000). In *Edmond*, the Court declined to apply the special needs doctrine and "suspend the usual requirement of individualized suspicion where the police [sought] to employ a checkpoint primarily for the ordinary enterprise of investigating crimes." *Id.* at 44. *See also* Maryland v. King, 133 S. Ct. 1958, 1978 (2013) ("So the Court has insisted on some purpose other than 'to detect evidence of ordinary criminal wrongdoing' to justify these searches in the absence of individualized suspicion.").

[172] *Von Raab*, 489 U.S. at 662.

[173] *King*, 133 S. Ct. at 1979–80. In reaffirming the special needs doctrine the Court stated: "[T]he search here at issue differs from the sort of programmatic searches of either the public at large or a particular class of regulated but otherwise law-abiding citizens that the Court has previously labeled as "'special needs'" searches." *Id.* at 1978 (citing Chandler v. Miller, 520 U.S. 305, 314 (1997)). "The special needs cases, though in full accord with the result reached here, do not have a direct bearing on the issues presented in this case, because unlike the search of a citizen who has not been suspected of a wrong, a detainee has a reduced expectation of privacy." *Id.*

[174] *Id.* at 1979–80.

[175] The court found that:

> [T]he Act provides statutory protections that guard against further invasion of privacy. As noted above, the Act requires that "[o]nly DNA records that directly relate to the identification of individuals shall be collected and stored." No purpose other than identification is permissible: "A person may not willfully test a DNA sample for information that does not relate to the identification of individuals as specified in this subtitle." This Court has noted often that "a 'statutory or regulatory duty to avoid unwarranted disclosures' generally allays . . . privacy concerns." The Court need not speculate about the risks posed "by a system that did not contain comparable security provisions." In light of the scientific and statutory safeguards, once respondent's DNA was lawfully collected the STR analysis of respondent's DNA pursuant to CODIS procedures did not amount to a significant invasion

To illustrate the impermissibly overbroad use of the special needs doctrine in national security cases, assume the NSA, under the authority of FISA and the special needs doctrine, collects the metadata of all Verizon customers for national security reasons. After the acquisition of the data, the government decides to investigate a foreign target it suspects is engaging in terrorist activity. During the investigation of the foreign target, the government reads emails between the foreign target and an American citizen and discovers that the American citizen is involved in the sale of drugs. Although this investigation is permissible under FISA, the special needs doctrine should not sanction the government's subsequent use of this evidence in a prosecution unrelated to national security involving the sale of drugs.

Constitutional scholar Owen Fiss believes that an expansion and application of the special needs doctrine in terrorism cases is a mistake, and an exception to the warrant requirement for extraordinary crimes would be prone to great abuse.[176] Legal scholar William J. Stuntz, however, believed that "[d]ifferent crimes give rise to different government interests, which in turn should lead to different Fourth Amendment standards."[177] The "worst crimes are the most important ones to solve, the ones worth paying the largest price in intrusions on citizens' liberty and privacy."[178] Supreme Court precedent supports this

> of privacy that would render the DNA identification impermissible under the Fourth Amendment.

Id. (internal citations omitted).

As the Court noted in *Skinner v. Ry. Labor Execs. Ass'n.*, an "essential purpose of a warrant requirement" is to assure that citizens' privacy rights are not violated through arbitrary and random searches by the government. *Skinner*, 489 U.S. at 621–22 (1989). By requiring that all employees involved in an accident be tested, the regulations at issue left virtually no discretion in the hands of government and, thus, no decision for a magistrate to make. *Id.* at 622.

[176] Fiss, *supra* note 152, at 28–29 (2012) ("The government can always claim that it is seeking to prevent an extraordinary crime and then defend that claim on the basis of knowledge that it alone has.").

[177] William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 849 (2001). Stuntz believed that in a homicide investigation, for example, probable cause should be enough to justify the search of a home without a warrant. *Id.* at 852. In fact, he stated, "perhaps a standard lower than probable cause would be appropriate. Meanwhile, for less-than-serious drug cases—anything associated with marijuana would be a good example—probable cause and a warrant should perhaps not be enough." *Id.*

[178] *Id.* at 875. In *Welsh v. Wisconsin*, the police, without obtaining a warrant, went to the defendant's home, gained entry and arrested him for driving under the influence of

view.

A policy that diminished Fourth Amendment standards, justifiable under certain well-defined circumstances, certainly makes sense in the area of national security. The April 15, 2013 Boston Marathon terrorist attack provides a perfect example. Police officers, with neither warrant nor cause, went door-to-door looking for the suspect.[179] However, the admissibility of evidence obtained during these searches must meet the reasonableness standard of the Fourth Amendment. Evidence of this kind should be inadmissible in subsequent prosecutions for crimes not pertaining to national security without a separate privacy analysis.

Because the special needs doctrine states that an intrusion on privacy is justified by a government need to ensure public safety, a tailored yet warrantless search of data on the cloud may be permitted, under certain circumstances, to ensure national security.[180] The circumstances outlined in the special needs doctrine, after all, are comparable to the "exigent circumstances" set forth in *Riley*. The *Riley* Court held that warrantless searches are justified under the exigent circumstances doctrine when the "needs of law enforcement are so compelling" that it makes such a search reasonable.[181] Similarly, under the special needs doctrine, warrantless searches are justified when the

an intoxicant. Welsh v. Wisconsin, 466 U.S. 740, 743 (1984). The Court held that the Fourth Amendment prohibited the warrantless, nighttime entry into the petitioner's home to arrest him for a civil, non-jailable traffic offense, as standards regulating a murder investigation should not be the same as in a drunk driving investigation. *Id.* at 753. It reasoned that "an important factor to be considered when determining whether any exigency exists is the gravity of the underlying offense for which the arrest is being made." *Id.*

[179] Philip Bump, *Boston's Door-to-Door Searches Weren't Illegal, Even Though They Looked Bad*, ATLANTIC WIRE (Apr. 22, 2013, 5:51 PM), http://www.theatlanticwire.com/national/2013/04/boston-door-to-door-searches-legal/64461; *see also* Katy Waldman, *Can the Police Search My Home for a Bomber? Why the Door-to-Door Manhunt for Dzhokhar Tsarnaev Doesn't Violate the Constitution*, SLATE (Apr. 19, 2013), http://www.slate.com/articles/news_and_politics/explainer/2013/04/boston_bomber_manhunt_is_the_watertown_door_to_door_search_by_police_for.html.

[180] *See, e.g.*, *Skinner*, 489 U.S. 602; Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989); City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

[181] Riley v. California, 134 S. Ct. 2473, 2492 (2014) (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978)). Examples of such situations include the need to prevent imminent destruction of evidence, pursue a fleeing suspect, and to assist people who are seriously injured or are threatened with immediate injury. *Id.* at 2494.

"need to discover . . . latent or hidden conditions, or to prevent their development, is sufficiently compelling to justify the intrusion on privacy entailed by conducting such searches without any measure of individualized suspicion."[182] Thus, in order to satisfy both the special needs doctrine and the exigent circumstances doctrine, the actions of the state must be reasonable and compelling.[183] Therefore, as proposed in this article, a unique analysis must be applied to every case rather than a broad rule.

Though President Obama has stated, "[y]ou can't have 100 percent security and also then have 100 percent privacy and 0 percent inconvenience,"[184] the state must strike the proper balance between

[182] *Von Raab*, 489 U.S. at 668.

[183] *Id.*; *Riley*, 134 S. Ct. at 2492; Lebron v. Sec'y, Fla. Dep't of Children and Families, 710 F.3d 1202, 1207–08 (11th Cir. 2013).

[184] Matt Spetalnick & Steve Holland, *Obama Defends Surveillance Effort as 'Trade-off' for Security*, REUTERS (June 7, 2013, 11:42 PM), http://www.reuters.com/article/email/idUSBRE9560VA20130608. Most Americans appear willing to sacrifice some liberty for security. *See* Heather Kelly, *Some Shrug at NSA Snooping: Privacy's Already Dead*, CNN (June 9, 2013), http://www.cnn.com/2013/06/07/tech/web/nsa-internet-privacy. A national survey conducted in April 2013 by CNN, Time and ORC International revealed "40% of respondents were willing to give up some of their civil liberties for increased security." *Id.* Even more revealing, a survey conducted by the Allstate/National Journal Heartland Monitor just days before the PRISM revelations, "found that 85% of Americans already believed their phone calls, e-mails and online activity were being monitored." *Id.*

However, a Washington Post-ABC News poll released the week of July 22, 2013, showed that 39 percent of those questioned say it is more important for the federal government not to intrude on personal privacy than to investigate terrorist threats. *July 2013 Washington Post-ABC News National Poll*, WASH. POST, http://apps.washingtonpost.com/g/page/politics/july-2013-washington-post-abc-news-national-poll-national-politics-trayvon-martin/327 (last visited Jan. 6, 2015). That was the highest number since the question was first asked in 2002, when it was 18 percent. Jon Cohen & Dan Balz, *Poll: Privacy Concerns Rise After NSA Leaks*, WASH. POST (July 24, 2013), http://www.washingtonpost.com/politics/poll-privacy-concerns-rise-after-nsa-leaks/2013/07/23/3a1b64a6-f3c7-11e2-a2f1-a7acf9bd5d3a_story.html.

Scott Shane, *Spy Agencies Under Heaviest Scrutiny Since Abuse Scandal of the '70s*, N.Y. TIMES, July 25, 2013, at A15, *available at* http://www.nytimes.com/2013/07/26/us/politics/challenges-to-us-intelligence-agencies-recall-senate-inquiry-of-70s.html ("With alarm over the threat of terrorism in slow decline despite the Boston Marathon attack in April, Americans of both parties appear to be no longer willing to give national security automatic priority over privacy and civil liberties.").

Wesley MacNeil Oliver states, "We are no longer a private people. We live out loud. Perhaps quite naturally, there is no one poised to vigorously represent privacy concerns in these new technologies." Oliver, *supra* note 74, at 989.

privacy and national security. Although there is precedent for surveillance of this nature during national emergencies, courts should prevent the government from using data acquired during terrorism investigations in later criminal prosecutions that do not involve an overriding public danger.[185] Evidence discovered by the government during online surveillance that does not relate to terrorism should be inadmissible in prosecutions of those unrelated matters.

VI. CONCLUSION

"Prayin' for Rain Through a Cloud of Dust"[186]

Due to Congress's focus on national security rather than Fourth Amendment concerns, statutory protections have failed to ensure a proper balance between privacy and public safety.[187] Government access to material in the cloud should always be subject to a reasonableness review, consisting of weighing government interest in national security against an individual's interest in privacy.[188] Ohm states, "The new

See also Jose Felipe Anderson, *Big Brother or Little Brother? Surrendering Seizure Privacy for the Benefits of Communication Technology*, 81 MISS. L.J. 895, 911 (2012) ("The average citizen has lost so much control over their personal information that it may be impossible to reverse the trend.").

[185] *See, e.g.*, David T. Z. Mindich, *Lincoln's Surveillance State*, N.Y. TIMES, July 5, 2013, at A17, *available at* http://www.nytimes.com/2013/07/06/opinion/lincolns-surveillance-state.html (noting that while the massive NSA surveillance is alarming, it is not unprecedented). In 1862, the article notes, after President Abraham Lincoln appointed him secretary of war, Edwin M. Stanton requested and was granted sweeping powers, including total control of the telegraph lines. *Id.* "By rerouting those lines through his office, Stanton would keep tabs on vast amounts of communication, journalistic, governmental and personal." *Id.* "So it has been with many wars: a cycle of draconian measures followed by contraction." *Id.*

[186] BRAD PAISLEY, *Cloud Of Dust*, *on* WHO NEEDS PICTURES (Arista Nashville 1999).

[187] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); People v. Weaver, 882 N.Y.S.2d 357, 364–65 (N.Y. 2009); State v. Holden, 54 A.3d 1123, 1133 (Del. Super. 2010).

Slobogin urges the adoption of a "proportionality principle" which "would state that, for every government action that implicates the Fourth Amendment, government must demonstrate 'cause'—defined as the level of certainty that evidence of wrongdoing will be found" proportional to the invasiveness of the search. Slobogin, *supra* note 84, at 15. Under the proportionality principle, less invasive searches would be permissible, such as police viewing of public activities. *Id.* Conversely, law enforcement personnel would have to demonstrate a high degree of cause when conducting virtual searches that are as intrusive as an entry into the home. *Id.*

[188] Fourth Amendment scholar Thomas K. Clancy suggests "any intrusion with the purpose of obtaining physical evidence or information, either by a technological device

constitutional lodestar, power, is the Fourth Amendment's third act."[189] Property and privacy "were both imperfect proxies for what the amendment actually protects."[190] "Power seems to be the amendment's essence, not merely a proxy for something deeper."[191]

The judiciary must continue to act as a buffer of reason and careful thinking against the vast and insistent power of law enforcement.[192] With little judicial oversight, the government is now able to reach beyond the boundaries of the Fourth Amendment. "The privacy and dignity of our citizens is being whittled away in sometimes

---

or the use of the senses into a protected interest should be considered a search, and, therefore, must be justified as reasonable." Thomas K. Clancy, *What is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 3 (2006).

Cynthia Lee, in her article *Reasonableness with Teeth*, states: "Even though it still treats as reasonable both searches conducted pursuant to a warrant and searches that fall within a well-established exception to the warrant requirement, the modern Court has increasingly abandoned the warrant preference view." Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133 (2012). "Instead of interpreting the Fourth Amendment as expressing a preference for warrants, the modern Court reads the text of the Fourth Amendment as simply requiring reasonableness." *Id.* at 1135.

Slobogin states: "Given the huge amount of information that virtual searches provide about everyone's activities and transactions, traditional physical searches — with their cumbersome warrant and probable cause requirements — are much less necessary than they used to be." Slobogin, *supra* note 84, at 9; *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 818–19 (1994).

[189] Ohm, *supra* note 15, at 1337.

[190] *Id.* at 1338.

[191] *Id. See also* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 757 (1989) (cautioning that the government's need to know should be carefully balanced against a citizen's need for the government not to know).

[192] Greenwald & MacAskill, *supra* note 45. A revolution in software technology "has transformed the N.S.A., turning it into the virtual landlord of the digital assets of Americans and foreigners alike." James Risen & Eric Lichtblau, *How the U.S. Uses Technology to Mine More Data More Quickly*, N.Y. TIMES, June 9, 2013, at A1, *available at* http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html. The targets of the surveillance are foreigners, but Americans' data can be swept into the database when they communicate with people overseas. Alicia Parlapiano, *Comparing Two Secret Surveillance Programs*, N.Y. TIMES (June 7, 2013), http://www.nytimes.com/interactive/2013/06/07/us/comparing-two-secret-surveillance-programs.html. The FISC, Congress and the White House have oversight. *Id.*

As Judge Kozinski stated, "We are taking a giant leap into the unknown, and the consequences for ourselves and our children may be dire and irreversible." United States v. Pineda–Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting).

imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole," the danger of incremental encroachments to the Fourth Amendment become apparent.[193]

Measures regulating technology need to adhere even more strictly to Fourth Amendment standards of reasonableness. Though Supreme Court jurisprudence does not provide a bright line test, recent decisions, like *Riley*, act as a compass for future decisions by pointing toward Fourth Amendment protection for digital data. Even though the nature of information storage and recording has evolved, the constitutional principles governing privacy and the use of information by police should not be swept aside. The government's ability to access content-based data stored in the cloud without adequate judicial supervision infringes upon our citizens' personal freedoms and should not be allowed absent exigent circumstances or a warrant issued upon probable cause, as Supreme Court jurisprudence has required for over half a century.

[193] Osborn v. United States, 385 U.S. 323, 343 (1966).