Golden Gate University Law Review

Volume 43 | Issue 2 Article 4

April 2013

Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices

Mark Wilson
Golden Gate University School of Law

COMMENT

CASTLE IN THE CLOUD: MODERNIZING CONSTITUTIONAL PROTECTIONS FOR CLOUD-STORED DATA ON MOBILE DEVICES

*MARK WILSON**

For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that—either now or in the uncertain future—patterns we leave behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts. We lose our individuality, because everything we do is observable and recordable.[1]

INTRODUCTION

Eighty-five years ago, Justice Louis Brandeis described "the right to be let alone" as "the right most valued by civilized men."[2] That right is now under attack, and people themselves—all of us—are the attackers.

* J.D. Candidate, 2013, Golden Gate University School of Law; B.A. 2005, Miami University (Ohio). I wish to thank my advisors for this Comment, Professors Laura Cisneros and Robert Calhoun of Golden Gate University School of Law, as well as everyone around me who has graciously endured my talking about this issue for the past few years.

[1] Bruce Schneier, *The Eternal Value of Privacy*, WIRED (May 18, 2006), www.wired.com/politics/security/commentary/securitymatters/2006/05/70886.

[2] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

Chief Judge Alex Kozinski of the U.S. Court of Appeals for the Ninth Circuit announced the death of the Fourth Amendment, blaming technology for its demise: "Our weapon of choice? Most recently, the smartphone, which, with our collective blessing, allows law enforcement to monitor our real-time geographic location."[3] As Judge Kozinski sees it, we have surrendered a disproportionate amount of privacy for a little convenience.[4]

Though the Fourth Amendment prohibits unreasonable searches of "persons, houses, papers, and effects,"[5] its author, James Madison, could never have contemplated that a search of a person could simultaneously encompass effects located in another state. The rise of smart phones—cell phones with persistent Internet connections[6]—has injured the Fourth Amendment, but Judge Kozinski's eulogy may be premature.

Among the new technologies with the potential to adversely impact privacy is cloud computing. In a cloud computing environment, a user's documents are stored on a remote computer system operated and controlled by a third party.[7] Two popular cloud computing applications, Apple's iCloud and Dropbox (from the company of the same name), market their software by pointing out the convenience they afford.[8] Apple boasts that its iCloud service synchronizes a variety of data, including documents and web browser history, to all of a user's devices with minimum setup.[9] Dropbox advertises that "[a]ny file you save to Dropbox also instantly saves to your computers, phones, and the Dropbox website."[10] Cloud computing is not merely a niche technology either: millions of people use Dropbox today.[11]

Convenient as this synchronization may be, it raises disturbing Fourth Amendment issues. It also raises confusing statutory issues under

---

[3] Alex Kozinski & Stephanie Grace, *Pulling Plug on Privacy: How Technology Helped Make the Fourth Amendment Obsolete*, THE DAILY (June 22, 2011), www.thedaily.com/page/2011/06/22/062211-opinions-oped-privacy-kozinski-grace-1-2/.

[4] *Id.*

[5] U.S. CONST. amend. IV.

[6] A "smart phone" does not have a standardized definition, but it appears accepted in the field that a smart phone "combines the functions of a cellular phone and a handheld computer in a single device." Michael Juntao Yuan, *What Is a Smartphone*, O'REILLY WIRELESS DEVCENTER, www.oreillynet.com/wireless/2005/08/23/whatissmartphone.html (last visited Dec. 12, 2012).

[7] ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 05/2012 ON CLOUD COMPUTING, WP 196, at 5 (July 1, 2012), *available at* ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[8] DROPBOX, TOUR, www.dropbox.com/tour/0 (last visited Jan. 29, 2012).

[9] APPLE, ICLOUD FEATURES, www.apple.com/icloud/features/ (last visited Feb. 24, 2013).

[10] DROPBOX, FEATURES, www.dropbox.com/features (last visited Nov. 18, 2011).

[11] In January 2010, Dropbox announced that 4 million people used its service. *See* Robin Wauters, *Dropbox Announces 4 Million Users, Hires a VP from Salesforce*, TECHCRUNCH (Jan. 20, 2010), techcrunch.com/2010/01/20/dropbox-4-million-user/.

a federal statute known informally as the Stored Communications Act (SCA).[12] Enacted as part of the Electronic Communications Privacy Act (ECPA),[13] SCA created a separate standard for obtaining a search warrant when the "effects" to be searched are electronic communications transmitted to, and stored with, a "remote computing service."[14]

In 1986, when digital information still resided in large data centers, the Fourth Amendment problem was limited, as the data stored in data centers were not readily transportable.[15] Today, however, "essentially unlimited" online storage[16] allows users not only to store copious amounts of data, but also to access those data from multiple places, including a mobile phone.[17] As some courts have held that police may search the contents of a cellular phone incident to a lawful arrest,[18] the question becomes how deep into a phone's data the police can go, and whether that search is limited to information stored on the phone or information that is *accessible* by the phone.

Arguably, information accessible by a mobile device but stored on a third-party server is an "electronic communication" within the meaning of the SCA.[19] To a police officer trying to search a mobile device incident to an arrest, this presents a problem; cloud-stored information might be protected by the Fourth Amendment, but if it is not, the information may fall within the ambit of the SCA. If the former, then absent an exception to the warrant requirement, police must obtain a warrant to search cloud-stored documents accessible by a phone. If the latter, then more complex calculations become necessary. If the data were in storage for less than 180 days, a warrant supported by probable cause may be required.[20] But if the data were stored for more than 180 days, a warrant is optional because police can obtain an administrative

---

[12] Electronic Communications Privacy Act of 1986 tit. II, Pub. L. No. 99-508, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C.A. §§ 2701-2710 (Westlaw 2012)).

[13] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

[14] 18 U.S.C.A. § 2711(2) (Westlaw 2012).

[15] *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 17-18 (statement of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, Inc.), *available at* judiciary.house.gov/hearings/printers/111th/111-149_58409.pdf.

[16] *Id*. at 24 (statement of Mike Hintze, Associate General Counsel, Microsoft Corporation).

[17] *Id*. at 10 (statement of Edward W. Felten, Director, Center for Information and Technology Policy, Princeton University).

[18] *See, e.g.*, People v. Diaz, 244 P.3d 501 (Cal. 2011).

[19] Such communication is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C.A. § 2510(12) (Westlaw 2012); *see also id.* § 2510(14), (17).

[20] 18 U.S.C.A. § 2703(a) (Westlaw 2012).

subpoena, which can be issued based on something less than probable cause.[21] Or the information may not be protected at all.

If the SCA does not govern a search incident to arrest, current law requires complex calculations that could result in the exclusion of evidence if police are too liberal when searching, or the potential loss of evidence if they are too conservative. The exclusionary rule, designed by the Supreme Court in *Weeks v. United States*, and made applicable to the states in *Mapp v. Ohio*, is a Fourth Amendment enforcement mechanism.[22] The remedy for evidence obtained in violation of the Fourth Amendment is to bar the prosecutor from using that evidence against the accused.[23] Equally compelling is the prosecution's interest in preventing a suspect from destroying evidence on his person or nearby, leading to the search-incident-to-arrest[24] and automobile-search[25] doctrines.[26] While the law is clear that police may search a suspect's person incident to arrest, including any containers located thereon,[27] the law is unclear as to whether a cell phone is just another container or a different beast with a separate set of search rules.[28] The end result of this needlessly complex flowchart will be a rise in motions to exclude evidence at criminal trials. Police on the beat must be able to make evidentiary decisions at a moment's notice.[29] This leads to disparate enforcement of the law.

---

[21] *Id.*

[22] United States v. Calandra, 414 U.S. 338, 348 (1974) ("In sum, the rule is a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.").

[23] Weeks v. United States, 232 U.S. 383, 393 (1914) ("If letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the 4th Amendment, declaring his right to be secure against such searches and seizures, is of no value, and, so far as those thus placed are concerned, might as well be stricken from the Constitution."); *see* Mapp v. Ohio, 367 U.S. 643, 654 (1961).

[24] Chimel v. California, 395 U.S. 752, 763 (1969).

[25] Arizona v. Gant, 556 U.S. 332, 343-44 (2009).

[26] *See id.* at 339 (describing the search-incident-to-arrest doctrine as "protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy").

[27] United States v. Robinson, 414 U.S. 218, 235-36 (1973).

[28] *See, e.g.*, People v. Diaz, 244 P.3d 501, 505-06 (Cal. 2011) (holding that a cell phone is searchable like any other container on suspect's person); State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) (holding that a cell phone is not akin to containers from prior case law and could not be searched without a warrant); Hawkins v. State, 704 S.E.2d 886, 891-92 (Ga. 2010) (holding that, even though a cell phone is like a container, that characterization allows police to search some, but not all, of the files on the device).

[29] *Robinson*, 414 U.S. at 235 ("A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick ad hoc judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search.").

This Comment argues that the current state of Fourth Amendment law vis-à-vis searching cloud-stored documents on a mobile device is untenable.[30] Part I of this Comment defines cloud storage and cloud computing, and it provides background information on the SCA. Part II discusses the intricacies of applying the SCA to computers and email, which is to date the best analog for applying the SCA to cloud computing. Part III details the legislative and judicial solutions to the problems raised by new technology and concludes that, while new legislation is the most desirable response, in the meantime courts must rethink their notions of what it means to search a mobile device. If either the legislature or the judiciary can reform a troubled Fourth Amendment jurisprudence as it relates to new technology, hope remains that reports of the Fourth Amendment's death have been greatly exaggerated.

I. BACKGROUND

The Fourth Amendment does not require the government to obtain a warrant in all situations; only otherwise "unreasonable searches and seizures" require a warrant issued "upon probable cause."[31] The United States Supreme Court addressed the question of what constituted an unreasonable search in the 1928 case *Olmstead v. United States*.[32] Roy Olmstead was accused of leading a conspiracy to import liquor into the United States during Prohibition.[33] Federal prohibition officers had intercepted Olmstead's telephone conversations by tapping into the telephone wires outside his office.[34] This was accomplished without trespassing onto Olmstead's property.[35] In upholding Olmstead's conviction, the Supreme Court found it dispositive that the government listened to his phone conversations "without trespass upon any property

[30] What this Comment will *not* do is discuss privacy expectations relating to social media applications (e.g., Facebook, Twitter) that may be accessible by a mobile device. In addition to being beyond the scope of a discussion of cloud-stored communications, it is highly likely that information posted to Facebook or Twitter carries with it no privacy expectation, as the user has intentionally placed the information on the Internet for all to see. *See, e.g.*, Bruce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J. L. & TECH. 12 (2011); Connie Davis Powell, *"You Already Have Zero Privacy. Get over It!" Would Warren and Brandeis Argue for Privacy for Social Networking?*, 31 PACE L. REV. 146 (2011).

[31] U.S. CONST. amend IV.

[32] Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[33] *Id.* at 456.

[34] *Id.* at 456-57.

[35] *Id.* at 457.

of the defendants,"[36] emphasizing that the government violated the Fourth Amendment only if it interfered with the suspect's property.[37]

In 1967's landmark *Katz v. United States*, the Supreme Court reversed *Olmstead* when it held that "the Fourth Amendment protects people, not places."[38] Federal agents, believing that Charles Katz was illegally transferring wagering information over the phone, attached an electronic listening device to the outside of the phone booth in which Katz made the illegal calls.[39] Agents never interfered with the *inside* of the phone booth.[40] However, for the *Katz* Court, the relevant inquiry was not whether Charles Katz had a property interest in the phone booth (or, even if he did, whether federal agents had to "trespass" into the phone booth to listen to the conversation), but rather whether a person who "occupies [a phone booth], shuts the door behind him, and pays the toll" is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[41]

Justice John Marshall Harlan II, concurring in the judgment, took this new doctrine even further, articulating the familiar two-pronged test that remains the standard for determining when the government has engaged in a Fourth Amendment search:[42] "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[43] As technology has advanced, the Court has relied on this test in determining, for example, whether warrantless searches using pen registers,[44] heat-detection devices,[45] and aerial surveillance[46] violate the Fourth Amendment.

---

[36] *Id*.

[37] *Id*. at 466 ("Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure.").

[38] Katz v. United States, 389 U.S. 347, 351 (1967).

[39] *Id*. at 348.

[40] *Id*. at 352.

[41] *Id*.

[42] *See* Smith v. Maryland, 442 U.S. 735, 739 (1979) ("In determining whether a particular form of government-initiated electronic surveillance is a 'search' within the meaning of the Fourth Amendment, our lodestar is *Katz v. United States*." (footnote and citation omitted)); Kyllo v. United States, 533 U.S. 27, 32-33 (2001).

[43] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[44] *Smith*, 442 U.S. at 740.

[45] *Kyllo*, 533 U.S. at 34-35.

[46] California v. Ciraolo, 476 U.S. 207, 211 (1986).

A. DEFINING THE CLOUD

"The Cloud" is the popular name for any Internet-based location where data are stored.[47] "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[48] Beyond merely providing storage, "cloud computing" can also refer to distributing processing tasks among many computing resources and then delivering the output to a client computer over a network.[49] The network used to connect the elements of the Cloud can be private (used by a single organization), community (used by a set of specific individuals), public (usable by the general public), or a hybrid of the three.[50] The Cloud discussed throughout this Comment is a public cloud consisting of the public Internet and a secure connection to a cloud storage service used by a subscriber of the cloud-storage service.[51]

Cloud computing operates using a client-server architecture, where the server is a computer that stores and retrieves data, and a client—a computer or other device—requests data.[52] A cloud computing "server" actually consists of dozens or hundreds of computer servers arranged in a huge cluster.[53] This cluster of servers not only stores the data that clients access, but also contains applications that manage the data.[54] The cloud computing service maintains a copy of a user's files on the user's device (e.g., computer, smart phone, tablet) and the cloud application

---

[47] Walter S. Mossberg, *Learning About Everything Under the "Cloud,"* WALL ST. J., May 6, 2010, *available at* online.wsj.com/article/SB10001424052748703961104575226194192477512.html.

[48] LEE BADGER ET AL., NAT'L INST. OF STANDARDS & TECH., CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS 2-1 (May 2012), *available at* csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf.

[49] Ian Foster et al., Cloud Computing and Grid Computing 360-Degree Compared, IEEE Grid Computing Environments (2008), *available at* arxiv.org/pdf/0901.0131.pdf. For the purposes of this Comment, "cloud computing" will be limited to its storage implications.

[50] BADGER ET AL., *supra* note 48, at 2-2.

[51] Even though companies such as Dropbox or Google store data on their own servers, these networks are not considered "private," as the services are available to the general public. *See* PETER MELL ET AL., NAT'L INST. OF STANDARDS & TECH., THE NIST DEFINITION OF CLOUD COMPUTING 3 (Sept. 2011), *available at* csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[52] Jonathan Strickland, *How Cloud Computing Works*, HOWSTUFFWORKS, computer.howstuffworks.com/cloud-computing/cloud-computing.htm (last visited Feb. 24, 2013).

[53] *Id.*

[54] *Id.*

synchronizes these copies with the copies stored on the remote server whenever the files change.[55]

Cloud storage utilizes the storage capacity of off-site servers instead of the storage provided by the internal disks in a computer.[56] Mobile devices, and even some smaller laptop computers, have limited storage capacity due to their small size and their necessarily small internal disks.[57] Unlike a traditional computer, which stores its data on an internal hard drive, a mobile device like an iPhone often stores its data on a third-party server, accessing the data as necessary.[58] Thus, as non-computer mobile devices have become more popular, use of cloud-storage services has increased as a necessity.[59]

Users choose to store their information in the Cloud, and not on their computers, for a variety of reasons. Information may be stored in the Cloud as a backup, in case the user's computer is lost or damaged, making the information stored on the computer unrecoverable.[60] Businesses increasingly find cloud computing to be a cheap alternative to hosting large amounts of data and the requisite backup and retrieval hardware on-site.[61] But even beyond the Cloud's business solutions—disaster recovery and saving money—users of all types find it convenient to access cloud-stored information wherever they have an Internet connection.[62]

Cloud-stored information is typically encrypted, meaning it cannot be accessed without the password of the person who owns the information.[63] This does not mean, however, that the information can *never* be accessed by anyone but the owner. The Terms of Service (TOS) for Dropbox, one of the most popular file-storage services, explicitly state that its employees may "disclose to parties outside

---

[55] For a description of how several cloud-computing services work, *see generally* Roger Spoor & Arjan Peddemors, *Cloud Storage and Peer-to-Peer Storage: End-User Considerations and Product Overview*, SURFNET (2010), *available at* www6.surfnet.nl/nl/Innovatieprogramma's/gigaport3/Documents/EDS-3R%20Cloud%20and%20p2p%20storage-v1.1.pdf.

[56] Mossberg, *supra* note 47.

[57] *Id.*

[58] *Id.*

[59] Allan Hoffman, *Dropbox More Than a Convenience: Cloud Storage Service a Sign of the Times*, THE STAR-LEDGER (Mar. 9, 2012), *available at* www.nj.com/business/index.ssf/2012/03/dropbox_more_than_a_convenienc.html.

[60] *Why Is Online Storage Becoming So Popular?*, ONLINESTORAGE.ORG, www.onlinestorage.org/why-is-online-storage-becoming-so-popular/ (last visited Feb. 24, 2012).

[61] *Id.*

[62] *Online Storage vs. External Hard Drives*, ONLINESTORAGE.ORG, www.onlinestorage.org/online-storage-vs-external-hard-drives/ (last visited Feb. 24, 2013).

[63] *See, e.g.*, DROPBOX, HOW SECURE IS DROPBOX?, www.dropbox.com/help/27 (last visited Feb. 24, 2012).

Dropbox files stored in your Dropbox" for several reasons, one of which is to "comply with a law, regulation or compulsory legal request."[64] Apple's TOS for its iCloud service are substantially similar.[65]

B. THE STORED COMMUNICATIONS ACT

Integral to any examination of searches of electronically stored material is the Stored Communications Act of 1986 (SCA).[66] SCA was passed as part of an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which established the authority for federal wiretaps.[67] Congress passed the SCA as primitive forms of electronic communication became prevalent, fearing that a person who handed computer information to a third party "may be subject to no constitutional privacy protection."[68] The SCA contains a strange idiosyncrasy, however: data that have been in electronic storage for less than 180 days can be obtained only with a warrant issued using either the procedures described in the Federal Rules of Criminal Procedure or a state's warrant procedures.[69] Information that has been in storage for longer than 180 days, however, can be obtained using a federal or state administrative subpoena or a court order.[70] In order to obtain electronically stored data under a court order, a state or federal governmental authority must show "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[71]

The reason for this disparity can be found in the SCA's legislative history and the peculiarities of data storage at the time the SCA was passed. The Senate observed, in 1986, that most data storage providers erased users' information after three months "to ensure system integrity."[72] Consequently, it was unlikely that someone would need to store data with a third party for more than six months. Erasing user data every three months was likely due to the prohibitive cost of data storage

---

[64] DROPBOX, TERMS, www.dropbox.com/terms#privacy (last visited Feb. 24, 2012).

[65] APPLE, ICLOUD TERMS AND CONDITIONS, www.apple.com/legal/icloud/en/terms.html (last visited Feb. 24, 2012).

[66] Electronic Communications Privacy Act of 1986 tit. II, Pub. L. No. 99-508, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C.A. §§ 2701-2710 (Westlaw 2012)).

[67] SEN. REP. NO. 99-541, at 1 (1986).

[68] *Id.* at 3.

[69] 18 U.S.C.A. § 2703(a) (Westlaw 2012).

[70] *Id.* § 2703(b).

[71] *Id.* § 2703(d).

[72] SEN. REP. NO. 99-541, at 3.

in 1986.[73] Indeed, a contemporary magazine article noted, "Prices for hard disks in the 10- or 20-megabyte capacities range from $400 to $1,500 depending on access time, capacity, and other features."[74] Compare this to a modern hard disk, which has a storage capacity of 2 terabytes (approximately 100,000 times the capacity of a disk in 1986) and costs only about $100.[75] Congress is aware that the SCA's 180-day provision is problematic: two former U.S. Representatives observed that, when Congress passed the SCA in 1986,

> people assumed that emails remaining on a server were forgotten or unwanted, and it made some sense to impart a higher level of protection to newer emails stored for fewer than 180 days. But today, with the nearly limitless storage capability that online services provide, the emails we save on the server are often the ones that are most important to us.[76]

Combine the proliferation of cloud-stored data with the ubiquity and convenience of mobile devices, then add a dash of statutory language that even former members of Congress acknowledge is woefully out of date, and a recipe for constitutional disaster is cooked up as millions of Americans walk around town with personal data in their pockets that is readily available to law enforcement.

II. APPLYING THE SCA TO MOBILE DEVICES INCIDENT TO ARREST

Yet another wrinkle in the SCA involves the statute's application to a search incident to an arrest. The SCA's very existence, and Congress's desire to place stored communications within the purview of the Fourth Amendment, suggest that the SCA is the exclusive mechanism for law enforcement seeking to access stored communications. This would seem to preclude the use of the common-law doctrine of search incident to arrest. However, The SCA does not make it entirely clear whether a

---

[73] Scott Shane, *Data Storage Could Expand Reach of Surveillance*, N.Y. TIMES BLOG (Aug. 14, 2012, 5:50 PM), thecaucus.blogs.nytimes.com/2012/08/14/advances-in-data-storage-have-implications-for-government-surveillance/ ("Not so long ago, even the most aggressive government surveillance had to be selective: the cost of data storage was too high and the capacity too low to keep everything.").

[74] Selby Bateman, *The Future of Mass Storage*, COMPUTE! (Mar. 1986), *available at* www.atarimagazines.com/compute/issue70/054_1_THE_FUTURE_OF_MASS_STORAGE.php.

[75] AMAZON.COM, www.amazon.com/Western-Digital-Caviar-Desktop-WD20EARX/dp/B004VFJ9MK/ (last visited Feb. 24, 2012).

[76] Asa Hutchinson & Mickey Edwards, *Get a Warrant: Congress Must Act To Protect Privacy in Digital Age*, THE HILL (Oct. 25, 2011), thehill.com/opinion/op-ed/189737-get-a-warrant-congress-must-act-to-protect-privacy-in-digital-age-.

warrant is *always* necessary to seize the material within its purview.[77] While "it is not presumed that the common law is changed by statutory enactment; and statutes in derogation of the common law are strictly construed,"[78] the Supreme Court "has not simply frozen into constitutional law those law enforcement practices that existed at the time of the Fourth Amendment's passage."[79] Thus, it could be that the SCA may override the common law doctrine of search incident to arrest,[80] placing a Dropbox or iCloud user's documents outside the reach of such a search.

In *United States v. Robinson*, the United States Supreme Court held that when a person is searched incident to a lawful arrest, "It is the fact of custodial arrest which gives rise to the authority to search. . . ."[81] Indeed, in the case of a lawful custodial arrest, "a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment."[82] Cases post-*Robinson* have made fine distinctions as to how far outside the physical boundaries of a "person" police could go in a search incident to arrest.[83]

State courts have recently become the arena for disputes surrounding police searches of cell phones incident to arrest.[84] The arena is a mess. In *People v. Diaz*, the California Supreme Court decided that police may search the contents of a cell phone incident to a lawful arrest, although the case dealt solely with text messages stored on the phone.[85] Conversely, the Ohio Supreme Court held in *State v. Smith* that "because

---

[77] *See* 18 U.S.C.A. § 2703(a) (Westlaw 2012): "A governmental entity *may* require the disclosure . . . *only* pursuant to a warrant . . ." (emphasis added). This language suggests that the only way in which the government can obtain electronic communications, as defined by the SCA, is through the warrant procedures specified by the SCA.

[78] 2A NORMAN J. SINGER & J.D. SHAMBIE SINGER, STATUTES AND STATUTORY CONSTRUCTION § 45.12 (7th ed. 2007).

[79] Tennessee v. Garner, 471 U.S. 1, 13 (1985) (quoting Payton v. New York, 445 U.S. 573, 571 n.33 (1980)).

[80] The Supreme Court recognized the existence of such a doctrine at common law in *Weeks v. United States*, 232 U.S. 383, 392 (1914), *overruled on other grounds*, Mapp v. Ohio, 367 U.S. 643 (1961).

[81] United States v. Robinson, 414 U.S. 218, 236 (1973).

[82] *Id*. at 235.

[83] *See* United States v. Edwards, 415 U.S. 800, 804-09 (1974) (holding that taking Edwards's clothing in order to subject it to a lab analysis was not a search); United States v. Monclavo-Cruz, 662 F.2d 1285, 1290-91 (9th Cir. 1981) (holding that a purse is within an arrestee's immediate control, not an element of her clothing or person); United States v. Passaro, 624 F.2d 938, 944 (9th Cir. 1980) (holding that search of suspect's wallet was permissible as a search of his person incident to arrest); United States v. Castro, 596 F.2d 674, 677 (5th Cir. 1979) (holding that a search of Castro's wallet was permissible as a search of his person incident to arrest).

[84] *See, e.g.*, People v. Diaz, 244 P.3d 501 (Cal. 2011); Hawkins v. State, 704 S.E.2d 886 (Ga. 2010); State v. Smith, 920 N.E.2d 949 (Ohio 2009).

[85] *Diaz*, 244 P.3d at 505-06.

a person has a high expectation of privacy in a cell phone's contents, police must then obtain a warrant before intruding into the phone's contents."[86] The Court of Appeals of Georgia apparently decided to split the difference, holding in *Hawkins v. State* that police did not have authority to search the entire contents of a cell phone, but only those contents "that might reasonably contain the object of the search."[87] Federal courts are similarly divided over whether the contents of cell phones can be searched incident to a lawful arrest.[88]

Justice Werdegar, dissenting in *Diaz*, posited the very problem that this Comment addresses: "Never before has it been possible to carry so much personal or business information in one's pocket or purse. The potential impairment to privacy if arrestees' mobile phones and handheld computers are treated like clothing or cigarette packages, fully searchable without probable cause or a warrant, is correspondingly great."[89] But *Diaz* dealt only with the information stored on the phone itself.[90] Justice Werdegar's statements are even more applicable to the world of the Cloud, where the storage capacity is, for all practical purposes, infinite.

A. THE SCA AS APPLIED TO CLOUD COMPUTING

It is unclear what would happen if a court faced the issue of applying the SCA to cloud-based services accessible by a mobile device. There are two issues involved in searching a mobile device incident to arrest. First, as noted above, is the problem presented by *Diaz* and *Smith*: whether a mobile device can be searched incident to arrest without a warrant.[91] But another issue, yet unanswered, is whether cloud-stored documents, specifically, can be searched incident to an arrest on a mobile device, or any device that connects to the Cloud, and whether the SCA even applies to cloud-stored documents.

In answering this question, email provides the best available analogy. An email provider falls within the scope of the SCA's

---

[86] *Smith*, 920 N.E.2d at 955.

[87] *Hawkins*, 704 S.E.2d at 892.

[88] United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (holding that police had authority to examine contents of Finley's phone without a warrant); United States v. Hill, 2011 WL 90130, at *7 (N.D. Cal. Jan. 10, 2011) (holding that a cellular phone should be considered part of a person's clothing and thus subject to a warrantless search incident to arrest). *Contra* Schlossberg v. Solesbee, 844 F.Supp.2d 1165, 1169-71 (D. Or. 2012) (adopting *Smith* and *Park*'s holding due to the volume of information a cellular phone can hold); United States v. Park, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007) (holding that a cellular phone should not be considered part of a person's clothing "due to the quantity and quality of information that can be stored").

[89] *Diaz*, 244 P.3d at 514 (Werdegar, J., dissenting).

[90] *Id.* at 502-03 (majority opinion).

[91] *Id.* at 503; *Smith*, 920 N.E.2d at 950-51.

definition of a "remote computing service," as it provides "to the public . . . computer storage or processing services by means of an electronic communications system."[92] The legal protections, if any, of email rely on an analogy to postal mail, a field where privacy expectations are well-established.[93] The United States Court of Appeals for the Armed Forces noted, in *United States v. Maxwell*, that "[email] transmissions are not unlike other forms of modern communication. We can draw parallels from these other mediums."[94] As it stands now, case law surrounding the search of email is probably the best clue to where the law is going, and where the law should probably not go, involving a search of cloud-stored information accessible by a mobile device. If email is afforded blanket protection under the Fourth Amendment, then so too should cloud-stored data.

B. *UNITED STATES V. WARSHAK* FINDS A RIGHT TO PRIVACY IN EMAIL

The judiciary has been slow to recognize that electronic information should be afforded the same Fourth Amendment protections as other types of "real-world" data.[95] Recently, the Sixth Circuit recognized a Fourth Amendment right to the privacy in email stored with an Internet Service Provider (ISP) in *United States v. Warshak*.[96] Steven Warshak was accused of mail and bank fraud for operating a business that distributed herbal supplements for male sexual enhancement.[97] As part of its investigation, the United States procured 27,000 of Warshak's private emails using an administrative subpoena, which was permitted by the SCA.[98] Warshak sought to suppress these emails as the result of an illegal search.[99] The Sixth Circuit found that, while Warshak did have a Fourth Amendment right to privacy in the emails, because the government relied on the SCA in good faith, Warshak's conviction should not be reversed.[100] Nevertheless, the Sixth Circuit held, "to the

---

[92] 18 U.S.C.A. § 2711(2) (Westlaw 2012).

[93] *See* Brief of *Amici Curiae* Electronic Frontier Foundation, ACLU of Ohio Foundation, Inc., American Civil Liberties Union, & Center for Democracy & Technology Supporting the Appellee & Urging Affirmance at 4, United States v. Warshak, 631 F.3d 266 (2010) (No. 06-4092), *available at* www.eff.org/files/filenode/warshak_v_usa/warshak_amicus.pdf.

[94] United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996).

[95] *See id.* at 418 (holding that the sender of an email message has a right to the privacy of its contents).

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

[97] *Id*. at 274.

[98] *Id*. at 282.

[99] *Id*. at 281.

[100] *Id*. at 282.

extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[101]

Even though the *Warshak* court affirmed the trial court's judgment by holding that the government relied in good faith on the SCA's constitutionality, the court set a precedent for future email privacy cases in the Sixth Circuit.[102] What is most important about *Warshak* is its reasoning. Applying the *Katz* test, the court found that Warshak did have a subjective expectation of privacy in his emails: "Given the often sensitive and sometimes damning substance of his emails, we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view."[103]

The court also found, under the second prong of *Katz*, that this was a privacy expectation society recognized as reasonable.[104] The *Katz* Court, forty-three years earlier, based its decision in part on "the vital role that the public telephone has come to play in private communication."[105] The *Warshak* court applied this same criterion to email, concluding that:

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.[106]

Warshak's use of *Katz*'s language about the expanded role of telephones in communication suggests that a "ubiquity check" is folded into the second prong of the test. The fact that email in 2010 was as common a medium of communication as the telephone in 1967 bolsters the reasonableness of society's privacy expectation in email.

---

[101] *Id*. at 288.
[102] *Id*. at 292.
[103] *Id*. at 284 (footnote omitted).
[104] *Id*. at 285-86.
[105] Katz v. United States, 389 U.S. 347, 352 (1967).
[106] *Warshak*, 631 F.3d at 284.

Consequently, "[a]s some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise."[107] Thus, the more useful and potentially indispensable a technology becomes to personal communication, commercial communication, or both, the more it is afforded Fourth Amendment protection.[108]

If *Warshak* were merely a vanilla case of a warrantless search under the Fourth Amendment, that would be the end of it; "[t]he government may not compel a commercial [Internet Service Provider] to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."[109] But the Sixth Circuit had to face the SCA, which gave the government the authority (the government thought) to obtain Warshak's emails.[110] Although the Sixth Circuit found that Warshak had an expectation of privacy in his email, that expectation was irrelevant in the face of the government's good-faith reliance on the SCA, even though the Court found the SCA unconstitutional.[111]

Cloud computing, though, might be a different animal altogether. There are easy analogies to be made (and *Warshak* makes them in coming to its conclusion[112]) between email and traditional postal mail. Postal mail has a long and storied history of use, making it something that courts understand.[113] Email, like regular mail, is a transmission from one person to another.[114] The sender intends for only one person, the recipient, to ever read that transmission.[115] A cloud storage system, on the other hand, is more like a bank deposit box: its contents, though

---

[107] *Id.* at 286.

[108] "Wait a minute," the reader might say at this point, "what about the Court's opinion in *Kyllo v. United States*? Wasn't there an expectation of privacy there *because* a thermal imaging gun *was not* in common use? Doesn't ubiquity cut both ways, resulting in inconsistent application?" This Comment, as well as the SCA, deals only with communications and not intrusive physical searches per se. Thermal imaging guns are hardly "indispensable" to communication and do not play a vital role in private communication. Moreover, the Court's opinion in *Kyllo* had much more to do with the imaging gun's invasion of the home than with its invasion of privacy in general. *See* Kyllo v. United States, 533 U.S. 27, 37-41 (2001).

[109] *Warshak*, 631 F.3d at 288.

[110] *Id.* at 282.

[111] *Id.* at 290.

[112] *See id.* at 285-86 ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy." (*quoting* Jacobsen v. United States, 466 U.S. 109, 114 (1984))).

[113] Brief for Professors of Electronic Privacy Law & Internet Law as *Amici Curiae* Supporting the Appellee & Urging Affirmance at 13, United States v. Warshak, 631 F.3d 266 (2010) (No. 06-4092), *available at* www.eff.org/sites/default/files/filenode/warshak_v_usa/amicus_final_law_profs.pdf.

[114] *Warshak*, 631 F.3d at 285.

[115] United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996).

accessible by a third party, are intended to be viewed only by the owner of the deposit box.[116] Using Dropbox or iCloud to save a document does not entail the intent to transmit that document's contents from one person to another, but rather to store that document in a safe place for later retrieval by the person who put it there originally. Even under this premise, such a document still has Fourth Amendment protection.[117]

C. THE UNCERTAIN DEFINITION OF "ELECTRONIC STORAGE"

Even though the Fourth Amendment and its associated case law *should* circumscribe the boundaries of cloud-storage searches, statutes like the SCA complicate an already complicated area of the law. The SCA carves out exceptions for certain types of searches but not others.[118] In examining the propriety of searching cloud-stored files on a mobile device without a warrant, a threshold issue is whether these types of data fall within one of these exceptions.

The SCA defines "electronic storage" both as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[119] It is this second clause of the SCA's definition of electronic storage that causes trouble, because the language of the statute may actually exempt some types of cloud-stored data from protection.

In *Theofel v. Farey-Jones*, the Ninth Circuit had to decide whether email messages stored on an ISP's remote email server until delivery were in "electronic storage" in light of case law holding that undelivered

---

[116] *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121, 165-66 (2008) ("[O]ne does not engage the third party because one wants the intermediary to have access; that access is a required means of effectuating the customer's interests. The same can be said of the user of a storage locker, a rental property, or a safe deposit box. The customer's interest in making use of the service necessitates the involvement of the third party. Of course, the same may be said of the ISP customer; she engages with the ISP out of the desire to use its intermediary services."). *Warshak* cites to this article in order to demonstrate that stored email is akin not only to a postal letter, but also to any other thing entrusted to a third party for delivery or storage. *Warshak*, 631 F.3d at 288.

[117] *See* Brief for Professors of Electronic Privacy Law & Internet Law as *Amici Curiae* Supporting the Appellee & Urging Affirmance, *supra* note 113, at 13-14 ("[W]hen someone maintains personal property on a third party's premises, she retains an expectation of privacy in it, so long as the property is secured against others' access and the third party's right of access to the premises is limited.").

[118] *See* 18 U.S.C.A. § 2703 (Westlaw 2012) and its divergent treatment of information that is newer or older than 180 days. The SCA also narrowly circumscribes what falls within its scope. *See generally* 18 U.S.C.A. § 2510 (Westlaw 2012).

[119] 18 U.S.C.A. § 2510(17) (Westlaw 2012).

emails were in "temporary, intermediate storage."[120] Finding that the emails were "stored 'by an electronic communication service' within the meaning of" the SCA,[121] the Ninth Circuit determined that the second clause of the definition of electronic storage—that data stored by an electronic communication service be stored "for purposes of backup protection"—applies to data *only if* it is being stored *for the purpose* of being backed up.[122] Furthermore, this intent to store data for backup protection must be the motivating reason for storage and not just another possible reason for storage; in order to fall within the scope of the SCA, "the mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose."[123]

In the Ninth Circuit's view, a "backup" consists of "storing a message on an ISP's server after delivery [in order] to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer."[124] A "backup" under the SCA thus requires both temporary storage data coupled with an intent to store those data in case a user (or, as the court concedes, the ISP) needs to access it again.[125] A copy of data stored for any other reason is, conceivably, not protected.[126]

In an aside that was not applicable in *Theofel*, but could be applicable to future cloud computing cases, the *Theofel* court considered the possibility that "[a] remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes."[127] This musing describes the cloud computing dilemma perfectly. People use cloud services for a variety of reasons, including, but not limited to, backing up information.[128] A person could also store information in the Cloud for ease of access from multiple devices.[129] Under the Ninth Circuit's interpretation of the SCA, such a use of the Cloud would not fall within the scope of the SCA, because the data were not stored solely for "backup purposes."

---

[120] Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003).

[121] *Id.*

[122] *Id.* at 1076.

[123] *Id.*

[124] *Id.* at 1075.

[125] *Id.*

[126] *See id.* at 1076 ("[T]he lifespan of a backup is necessarily tied to that of the underlying message. Where the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages.").

[127] *Id.* at 1077.

[128] *Why Is Online Storage Becoming So Popular?*, *supra* note 60.

[129] *Id.*

When it comes to cloud computing, a file located on the remote servers of companies such as Dropbox is "not stored for backup purposes," but is in fact constantly updated as the Dropbox software, installed on a user's computer or smart phone, monitors the local file for changes and updates the server's copy as necessary.[130] Herein lies the problem: in the Ninth Circuit, any non-backup data stored with a remote computing service may very well fall outside the statute's scope. Given that Congress's intention in crafting the SCA was to bring certainty to a new, uncertain area of technology,[131] it is woefully ironic that the statute's own language puts the very data it sought to protect out of its reach.

The court's aside in *Theofel*—that a user could potentially store all of his or her data on a remote computer, meaning that it is not backed up[132]—has started to hit home. *United States v. Weaver* was a child-pornography prosecution in which the government subpoenaed the defendant's email from Microsoft, the operator of the Hotmail email service, pursuant to the less-stringent SCA requirement.[133] The question for the court was, as in *Theofel*, whether the emails in question were in "electronic storage" under the SCA: "If the emails the Government requested here are in electronic storage, Microsoft need not produce them without a warrant, but if they are held or maintained solely to provide the customer storage or computer processing services, Microsoft must comply with the Government's subpoena."[134]

In *Weaver*, however, the defendant did not download the emails to his computer; instead, he viewed them from Hotmail's web interface.[135] Therefore, the copy held by Hotmail was not merely a backup copy; it was the *only* copy, and in that case, "Microsoft [was] not storing [his] opened messages for backup purposes. Instead, Microsoft [was] maintaining the messages 'solely for the purpose of providing storage or computer processing services to such subscriber or customer.'"[136] The *Weaver* court nevertheless looked to the legislative history of the SCA and concluded that "if the Stored Communications Act drafters intended emails a user leaves on an email service for re-access at a later date to be

---

[130] Idilio Drago et al., Inside Dropbox: Understanding Personal Cloud Storage Services 3, International Measurement Conference (2012), www.tlc-networks.polito.it/oldsite/mellia/papers/DropboxImc12.pdf.

[131] SEN. REP. NO. 99-541, at 3 (1986).

[132] *Theofel*, 359 F.3d at 1077.

[133] United States v. Weaver, 636 F. Supp. 2d 769, 769-70 (C.D. Ill. 2009).

[134] *Id.*

[135] *Id.* at 772.

[136] *Id.*

covered by section 2702(a)(2), they also must have intended them to be covered by the Government's trial subpoena power."[137]

III. SOLUTIONS: SEEKING CERTAINTY IN AN UNCERTAIN WORLD

As Judge Kozinski pointed out in *United States v. Comprehensive Drug Testing, Inc.* (known popularly as the BALCO case), "It's no answer to suggest . . . that people can avoid these hazards by not storing their data electronically."[138] The Cloud is here to stay, and with it must come strong, clear privacy protections for cloud-stored data.

Consider the situation in which Susie Citizen is pulled over by the city police for a traffic violation. Officer Friendly looks up Susie's name on his police computer and finds that she has a valid, outstanding arrest warrant because she failed to show up in court pursuant to a misdemeanor littering citation. Officer Friendly performs a custodial arrest of Susie and finds her iPhone in her pocket. Because current law permits him to examine the contents of containers on her person, he slides the virtual slider to get to the phone's home screen.

Officer Friendly opens up the Pages application, a word processor. This application's documents are stored in Apple's iCloud, not on the phone. The first document that appears is a list of Susie's crack cocaine clients and their outstanding balances with Susie. At a motion to suppress this evidence, Susie argues that she had a reasonable expectation of privacy in the contents of her iPhone, and none of the case law deals with information obtained by police that was not stored on the phone.

In the Ninth Circuit, a document stored on a cloud service may or may not be searchable under the SCA, depending on the user's intent in placing the document in the Cloud in the first place. Different interpretations of the same statute do not make for efficient law enforcement, especially for police in the field, who must make split-second decisions. Failing to document relevant evidence might lead to its destruction by the suspect before a warrant can be obtained; examining evidence that is protected by the Fourth Amendment could lead to the exclusion of relevant evidence.[139] Because the law is in flux, it is hard for the "cop on the beat" to know what to do. "Clear rules announce ex ante what the police can and cannot do; so long as the

---

[137] *Id.* at 773. It is difficult to say, however, what Congress intended with regard to modern email storage in 1986, as modern email systems did not exist.

[138] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam).

[139] *See* discussion of the exclusionary rule, *supra*, note 23 and accompanying text.

police comply with the clear rules, the police will know that the evidence cannot be excluded."[140] Requiring police to go through a complex flowchart of possible options (e.g., whether a document has been stored for longer than 180 days or even if such a document is electronically stored) does no one—police or civilians—any good. There must be a clear set of rules that, "in most instances, makes it possible to reach a correct determination beforehand as to whether an invasion of privacy is justified in the interest of law enforcement."[141]

In terms of policies that police can follow, the solutions will be either legislative or judicial. As the SCA is a federal law, Congress would have to address the statute's deficiencies. Alternatively, courts could avoid the SCA altogether and opt for an approach based on *Katz*'s two-prong test.[142] Or courts could reasonably conclude that a cell phone with cloud accessibility is too much like a computer to permit police to search it without a warrant; such a request is not outrageous, as the Ohio Supreme Court reached that conclusion with phones that were not connected to the Internet.[143] Any resultant policy will have to be simple and straightforward.

A. AMENDING THE STORED COMMUNICATIONS ACT

As this Comment is being written, legal organizations like the ACLU, the Electronic Frontier Foundation (EFF), and the Digital Due Process Coalition are hard at work crafting legislation to update the SCA.[144] In May 2011, Senator Patrick Leahy introduced The Electronic Communications Privacy Act Amendments Act of 2011.[145] The bill would have eliminated the SCA's peculiar 180-day provision and would have mandated that the contents of stored communications be obtained pursuant to a probable-cause warrant.[146] However, the proposed legislation would have permitted an administrative subpoena to be used to obtain identification information, such as the subscriber's name, address, or telephone number.[147]

---

[140] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 528 (2007).

[141] *Id.* (quoting New York v. Belton, 453 U.S. 454, 458 (1981)).

[142] Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

[143] "Although cell phones cannot be equated with laptop computers, their ability to store large amounts of private data gives their users a reasonable and justifiable expectation of a higher level of privacy in the information they contain." State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009).

[144] DIGITAL DUE PROCESS COALITION (Oct. 14, 2012), digitaldueprocess.org.

[145] Electronic Communications Privacy Act Amendments Act, S. 1011, 112th Cong. (2011).

[146] *Id.* § 3.

[147] *Id.*

In introducing the bill, Senator Leahy noted that, "[u]nder the current law, a single e-mail could be subject to as many a four different levels of privacy protections, depending upon where it is stored and when it was sent."[148] This bill, however, does not clarify the meanings of phrases like "electronic storage."[149] It also would permit exceptions to disclosure, including delayed notification (a search-warrant technique in which the person whose data are the subject of the search is notified of the search only after it has taken place).[150]

Professor Orin S. Kerr has expressed a dislike for the judicial approach to crafting Fourth Amendment protection, noting that statutes have been historically more important in crafting Fourth Amendment policy than case law.[151] For example, he observes that the history of wiretapping law, from *Olmstead* to *Katz*, "has remained a primarily statutory field governed by statutory commands. Indeed, it turns out that very few cases in the history of wiretapping law have ruled that a wiretapping practice violated the Fourth Amendment."[152] Professor Kerr makes much of Chief Justice Taft's helpful suggestion to Congress at the end of *Olmstead*:

> Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment.[153]

After *Olmstead*, Congress took Chief Justice Taft's advice and passed the first federal wiretapping law in 1934.[154] Even post-*Katz*, Congress has "taken the lead" in creating statutory privacy rights more protective than those offered by the Fourth Amendment.[155]

The legislative approach would be ideal, as the legislature is in a position to create a rule governing a situation before it happens, while courts are necessarily reactive, responding only to a putative violation

---

[148] 157 CONG. REC. S3054-01 (daily ed. May 17, 2011) (statement of Sen. Patrick Leahy).

[149] Nowhere within S. 1011 is there an updated or clearer definition of "electronic storage," leaving open the problem from *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003). Where a document not stored specifically for backup purposes might not be protected by the SCA.

[150] Electronic Communications Privacy Act Amendments Act, S. 1011 § 4.

[151] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 839 (2004).

[152] *Id*.

[153] *Id*. at 845 (quoting Olmstead v. United States, 277 U.S. 438, 465 (1928)).

[154] *Id*.

[155] *Id*. at 855.

that has already happened.[156] Well-crafted legislation could resolve the SCA's problems, including the 180-day provision, as well as the ambiguity over what "electronic storage" is. Such legislation would recognize that data are placed in electronic storage *because* we wish to keep them safe. Legislative rules, and not a myriad of different judicial opinions, would ostensibly provide the stability that police need in order to operate.

Representative Zoe Lofgren of California recently introduced the ECPA 2.0 Act of 2012 into the House of Representatives. The Act would update the SCA by eliminating the 180-day distinction, requiring law enforcement to obtain a warrant for all electronically stored data.[157] Representative Lofgren's attempt to update the SCA is laudable, but its detractors are powerful. Senator Leahy's 2011 measure faced opposition from such groups as the National District Attorneys' Association and the National Sheriffs' Association.[158] The United States Department of Justice opposed changes to the ECPA on the ground that "changes could adversely affect the critical goal of protecting public safety and the national security of the United States."[159]

B. APPLYING *KATZ* AND TRADITIONAL SEARCH-INCIDENT-TO-ARREST CASE LAW

Legislation may not be forthcoming, or the resultant legislation could make things worse. Cloud-stored documents must be protected somehow, and in a scenario in which legislation is nonexistent, or fails to recognize a constitutional privacy right in cloud-stored data, the judiciary would have to provide the protection.

In the interplay between the Supreme Court and Congress, there is a period where the law is either unclear or undesirable; for example, post-*Olmstead*, there was a six-year period in which law enforcement could wiretap with abandon before Congress passed the first wiretapping laws.[160] Post-*Warshak*, the SCA is unconstitutional, inasmuch as it purports to allow officials to obtain email without a warrant, but only in

---

[156] *Id*. at 868.

[157] ECPA 2.0 Act, H.R. 6529, 112th Cong. § 2(a) (2012).

[158] Declan McCullagh, *Senate Delays Netflix, E-mail Privacy Fix After Cops Protest*, CNET (Sept. 20, 2012, 11:07 AM), news.cnet.com/8301-13578_3-57517033-38/senate-delays-netflix-e-mail-privacy-fix-after-cops-protest/.

[159] *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 5 (2011) (statement of James A. Baker, Associate Deputy Attorney General).

[160] Kerr, *supra* note 151, at 845.

the Sixth Circuit.[161] Justice Alito, concurring in *United States v. Jones*, observed that, in the absence of legislation, "the best that [the Court] can do" is apply existing Fourth Amendment jurisprudence in determining when there has been a search.[162] With the SCA already in existence, it is hard to say that there is no legislation governing the situation at issue; however, the SCA's deficiencies—especially where SCA provisions contradict the Fourth Amendment—are perhaps worse than having no legislation at all.

In the absence of legislation, *Katz* provides an adequate test for determining a person's privacy expectations in a new technology. The *Warshak* court implied that *Katz* includes a "future-proof" mechanism.[163] When deciding whether a privacy right in a new technology is a right that society is prepared to recognize as a reasonable, courts should examine "the vital role that the [new technology] has come to play in private communication."[164] In this way, complex new technology can be afforded Fourth Amendment protection by answering two simple questions: Did this person believe his or her communication transmitted by this technology was private? Does society think that is a reasonable belief?

There are benefits to applying *Katz* directly. The *Katz* test has been with us for more than forty years, meaning that police departments are familiar with it.[165] *Katz* alleviates the need for constant legislative updates, as the second prong—the objective expectation of privacy—automatically changes as society changes. Presumably, as a particular communications technology becomes more useful and ubiquitous, society's reliance on it increases, and so too does society's reasonable expectation that communications will remain private.[166] Under *Katz*, Officer Friendly's warrantless search was likely impermissible, as there was no exigency and society recognizes that Susie's expectation of privacy in storing her documents on Apple's iCloud is reasonable.

---

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

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

[163] *See Warshak*, 631 F.3d at 286 (6th Cir. 2010) ("As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise.").

[164] Katz v. United States, 389 U.S. 347, 352 (1967). Note that the inquiry here is focused on "communication" and not merely "storage" or "presence." Applying *Katz*'s future-proofing to *Diaz* and *Smith*, where the information physically resided on the mobile device, is another topic, for another day.

[165] Kerr, *supra* note 140, at 526-27.

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

Katz also has its problems, not the least of which is its inconsistent application.[167] Even though the *Katz* Court professed to have abandoned the old property-based notion of privacy from *Olmstead*, the Supreme Court has continued to invoke property law in Fourth Amendment cases in determining whether a search was unreasonable.[168] An officer relying on *Katz* might have no way of knowing, before conducting her or his search, whether the search was constitutional.

However, a court can sidestep the traditional search-incident-to-arrest doctrine altogether. This is why the various cell phone cases came to different results.[169] For every *Smith* (in which the Ohio Supreme Court said a warrant was required to search the contents of a phone), there is a *Finley* (in which the Fifth Circuit upheld the characterization of a cell phone as a searchable container found on the arrestee's person).[170] In cases where courts have decided that police can rifle through a cell phone's contents, it is the phone's *location*, rather than its *character*, that has been the benchmark.[171] That is, because Officer Friendly found the phone on Susie's person, prior case law suggests that every bit of data accessible by the phone, irrespective of its actual location, is fair game for a search.[172]

---

[167] Professor Kerr observes, "*Katz* is a Rorschach test. Its vague language can support a narrow or broad reading equally well." Kerr, *supra* note 151, at 822.

[168] *Katz*, 389 U.S. at 353 ("[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."). *Contra* Kyllo v. United States, 533 U.S. 27, 37 (2001) (use of a thermal imaging device was a search because it was a "physical invasion of the structure of the home"); United States v. Jones, 132 S. Ct. 945, 951-52 (2012) (holding that *Katz* did not overrule the common-law doctrine of trespass as applied to rendering a search reasonable under the Fourth Amendment). *See generally* Daniel Zamani, *There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones*, 38 HASTINGS CONST. L.Q. 169, 174-75 (2010).

[169] *See, e.g.*, People v. Diaz, 244 P.3d 501, 505-06 (Cal. 2011) (holding that a cell phone was searchable like any other container on suspect's person); Hawkins v. State, 704 S.E.2d 886, 891-92 (Ga. 2010) (holding that, even though a cell phone is like a container, that characterization does not give police carte blanche to examine all the files on the device, but it allows police to examine some files); State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) (holding that a cell phone was not akin to containers from prior case law and could not be searched without a warrant).

[170] State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009). *Contra* United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007).

[171] *See, e.g.*, *Finley*, 477 F.3d at 260 (cell phone found on a suspect's person is akin to a container found on a suspect's person).

[172] *Diaz*, 244 P.3d at 509 ("These arguments [that the court should distinguish between the phone and its contents] are inconsistent with the high court's decisions. Those decisions hold that the loss of privacy upon arrest extends beyond the arrestee's body to include 'personal property . . . immediately associated with the person of the arrestee' at the time of arrest.").

C. SIDESTEPPING *ROBINSON*: "TECHNOLOGY NEUTRALITY" AND UNDERSTANDING THAT A PHONE IS NOT A WALLET

Other than seeking legislative change, some scholars advocate an approach that might satisfy even a *Finley*-type court. Professor Kerr has suggested a principle of "technology neutrality," under which "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."[173] A typical search-and-seizure situation depends on the physical limits of an object. "A search incident to arrest includes the physically grabbable area near the arrestee, but generally no further. A search warrant must describe the physical place to be searched with particularity, generally approving searches the physical scale of a single home or property but rarely more."[174]

On the Internet, however, "electronic data has no inherent limitations on how much can exist, where it can be located, and where it can be stored."[175] This disconnect gives rise to a Fourth Amendment problem in terms of the Cloud, where there are no physical limitations. Searching cloud-stored documents on a mobile device can be accomplished in minutes and not the weeks it would take to search an equivalent amount of documents in the physical world.[176] Even though the phone is "physically grabbable," the data may not be—indeed, it is likely that the data are located in a different jurisdiction.[177]

Analogizing a phone to a wallet is not the result of a misunderstanding about whether a phone is a wallet, but rather the result of jurisprudence that has failed to keep up with the types of technologies that can transform a wallet-*sized* object into a file-cabinet-*type* object. Courts that look at the size and location of a mobile device (e.g., whether it is on the person, in a purse, or in the car seat next to the suspect) focus

---

[173] Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007 (2010); *see also ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, *supra* note 15, at 24 (statement of David Schellhase, Executive Vice President and General Counsel, Salesforce.com).

[174] Kerr, *supra* note 173, at 1014.

[175] *Id.*

[176] Police can use devices such as the Cellebrite UFED, the subject of an ACLU lawsuit in Michigan, to extract the entire contents of a cell phone within minutes. *ACLU Concerned over Michigan State Police Extracting Data from Cellphones*, L.A. TIMES (Apr. 21, 2011, 4:50 PM), latimesblogs.latimes.com/technology/2011/04/aclu-concerned-over-michigan-state-police-extracting-phone-data.html.

[177] *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, *supra* note 15, at 107 (written statement of Thomas B. Hurbanek, Senior Investigator, New York State Police Computer Crime Unit).

too much on what Professor Kerr calls the "inside/outside distinction," which defines the parameters of a Fourth Amendment search in terms of what a human being can generally see with his or her eyes:

> Outside spaces are open to visual observation. The officer can use the surveillance tool of his eyes to see what is there. In contrast, closed spaces are closed from visual observation; the officer cannot see what is inside the enclosure. To see what is behind the barrier, the officer needs to break into the house, jimmy open the car trunk, unseal the letter, or otherwise break through the physical barrier that blocks his eyes from being able to see evidence inside.[178]

The Internet has rendered this definition of a "search" as "break[ing] through the physical barrier" meaningless.[179] Technology neutrality does not look at the physical character of the device storing the information, but rather creates a blanket protection for "content," that is, the substantive information that a person seeks to protect.[180]

Not everyone believes in crafting a new rule for "electronic containers." Byron Kish, writing in *Catholic University Law Review*, argues that a cellular phone is a container because it "can physically hold objects, for example, in a hidden compartment" and also because it "contains electronic information that can be reproduced in physical form."[181] This view, however, also falls victim to the problems associated with creating analogies. A mobile device could be searched for hidden compartments containing tangible, real-world objects (like a scrap of paper), but that would not affect the files on the device or stored in the Cloud, and the cloud-stored information would be intact. As for reproduction in physical form, documents and photographs could be downloaded from the device and printed, but this would make little sense, as people use the Cloud to obviate the need for maintaining physical copies of documents.[182]

The Supreme Court, despite Judge Kozinski's pessimism, seems prepared to recognize that new technology requires new rules. The two concurrences in the recent *United States v. Jones* decision suggest as much: Justice Sotomayor noted that "the same technological advances that have made possible nontrespassory surveillance techniques will also

---

[178] Kerr, *supra* note 173, at 1011.

[179] *Id*. at 1017-18.

[180] *Id*. at 1020.

[181] Byron Kish, *Cellphone Searches: Works Like a Computer, Protected Like a Pager?*, 60 CATH. U. L. REV. 445, 469 (2011).

[182] Paul Mah, *Three Benefits of Saving Files in the Cloud*, IT BUSINESS EDGE (Nov. 28, 2012), www.itbusinessedge.com/blogs/smb-tech/three-benefits-of-saving-files-in-the-cloud.html.

affect the *Katz* test by shaping the evolution of societal privacy expectations."[183] Justice Alito, concurring separately, agreed with the ultimate outcome but doubted the utility of the majority's property-based approach, especially since the search method employed—a GPS tracking device—was so far removed from anything known at common law.[184]

Justice Alito's offhand comment about a tiny constable or the very large coach, in addition to being entertaining, is also instructive.[185] The analogies used in Fourth Amendment jurisprudence deal with size, location, or other attributes of the physical world and not enough with the nature or use of the thing searched.[186] Cloud-stored documents can, and should, be afforded constitutional protection from warrantless searches under a theory that the police could not search a warehouse or a closed file cabinet without a warrant.

Notwithstanding cases like *Finley*, courts appear to be prepared to acknowledge the differences between phones and cigarette packs, pagers, or footlockers. As the federal district court in Oregon recently observed,

> the storage capability of an electronic device is not limited by physical size as a container is. In order to carry the same amount of personal information contained in many of today's electronic devices in a container, a citizen would have to travel with one or more large suitcases, if not file cabinets.[187]

Attaching an Internet connection to this container expands the capacity by many orders of magnitude to the point where the analogy breaks down solely on a common-sense level. Quite simply, "[a]n analogy between a computer and a container oversimplifies a complex area of Fourth Amendment doctrine and ignores the realities of massive modern computer storage."[188]

---

[183] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

[184] *Id.* at 958 (Alito, J., concurring).

[185] *Id.* at 958 n.3 (responding to the majority's assertion that common law could have contemplated round-the-clock vehicle surveillance by noting, "The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.").

[186] *See* State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) ("Given their unique nature as multifunctional tools, cell phones defy easy categorization. On one hand, they contain digital address books very much akin to traditional address books carried on the person, which are entitled to a lower expectation of privacy in a search incident to an arrest. On the other hand, they have the ability to transmit large amounts of data in various forms, likening them to laptop computers, which are entitled to a higher expectation of privacy.").

[187] Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1169 (D. Or. 2012).

[188] Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J. L. & TECH. 75, 110 (1994).

Any protection of a mobile device's cloud-stored documents, however, would have to extend protection to documents or files stored on the phone itself. It "would simply be an unworkable and unreasonable rule" to require the police to ascertain the nature of a mobile device before deciding to search its contents.[189] Police in the field are charged with making split-second evidentiary decisions and cannot engage in an analysis of what type of device they are dealing with.[190]

In *United States v. Comprehensive Drug Testing, Inc.*, the Ninth Circuit cautioned: "Authorization to search *some* computer files therefore automatically becomes authorization to search all files in the same sub-directory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media."[191] Thus, any rule governing mobile devices must, of necessity, encompass *all* mobile devices, including smart phones like the iPhone and the Android phone, or the "dumb" cell phone of the recent past. Treating all mobile devices like a computer would more than fulfill the necessity for a clear rule. Once in an officer's possession, the necessity for the search incident to arrest—the fear of evidence destruction before a warrant can be obtained[192]—disappears, and a "neutral and detached magistrate"[193] can decide, pursuant to the Fourth Amendment, whether the phone should be searched.

This does not mean that the police must "avert their eyes" when presented with a phone upon which there may be an open and obvious text message indicating criminal activity.[194] The "plain view" doctrine can be, and has been, applied to searches of computers.[195] In *United States v. Carey*, police acting pursuant to a warrant to search for evidence

---

[189] United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009).

[190] United States v. Robinson, 414 U.S. 218, 235 (1973) ("A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick ad hoc judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search.").

[191] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam).

[192] *Robinson*, 414 U.S. at 234.

[193] Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972).

[194] Coolidge v. New Hampshire, 403 U.S. 443, 489-90 (1971). The "plain view" doctrine has never required the police to avoid using their senses; it has merely reinforced that police may not go on treasure hunts when faced with the prospect of juicy evidence.

[195] United States v. Williams, 592 F.3d 511, 521-22 (4th Cir. 2010) (holding that warrant authorizing police to search suspect's computer for evidence of harassment and making criminal threats "impliedly authorized" police to open every file on the computer, at least to determine "whether the file fell within the scope of the warrant's authorization," meaning "any child pornography viewed on the computer or electronic media may be seized under the plain-view doctrine"); *see also* James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809 (2011).

of drug trafficking instead found child pornography on Carey's computer.[196] A police search of the "closed files," the court held, was not constitutional because the closed files (though not the first open file that initiated the search) were not in plain view.[197] If we must make analogies, then let us conclude that a smart phone is more like a computer than a pack of cigarettes. A pack of cigarettes cannot contain the contents of a diary without sacrificing its size. An iPhone, on the other hand, could contain the collected works of Shakespeare.

CONCLUSION

Convenient technologies are not flashes in the pan. "Electronic storage and transmission of data is no longer a peculiarity or a luxury of the very rich; it's a way of life."[198] Convenience breeds use, and with use, necessity. The telegraph, telephone, email, and cell phone have all had their time as essential to individual lives and worldwide communications. Increasingly, even voice communication on cell phones has taken a backseat to data transfers.[199] The Cloud takes communication technology to the next level. It enables us to take our "papers" with us wherever we go, but in a way that is nothing like a briefcase. Quite literally, a person with a mobile device and cloud storage can access every document she or her has ever written and every photo she or he has ever taken, from anywhere in the world so long as there is an Internet connection. The limitations of physical space no longer apply. For example, I could save this Comment to Dropbox and edit it on my iPhone from a Maui beach if necessary.[200] It appears, however, that a combination of uncertain jurisprudence and antiquated statutes have conspired to grant cloud-stored documents less protection than the Fourth Amendment demands.

The SCA, though well intentioned, may pave the road to the demise of privacy as electronically stored and transmitted communication becomes ever more important. The SCA needs to be amended, and well-crafted legislation could solve the problems of ambiguity and the questionable 180-day requirement that the Sixth Circuit found unconstitutional. Without a functioning SCA, however, there must be

---

[196] United States v. Carey, 172 F.3d 1268, 1272-73 (10th Cir. 1999).

[197] *Id.* at 1273.

[198] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam).

[199] Jenna Wortham, *Cellphones Now Used More for Data Than for Calls*, N.Y. TIMES, May 14, 2010, at B1, *available at* www.nytimes.com/2010/05/14/technology/personaltech/14talk.html.

[200] Sadly, the University would not provide travel expenses to permit me to prove that this was true.

some way to determine whether cloud-stored information is constitutionally protected. And the Cloud is only one new technology that is changing how people live and work, while simultaneously creating headaches for law enforcement, which is forced to operate under rules based on eighteenth-century modes of living. Technology that cannot even be conceived of yet will be subject to ossified regulation that addresses a very narrow, and currently arbitrary, aspect of the data: whether they were stored for more than 180 days.

In the absence of legislation, the judiciary must intervene and determine that mobile devices, and the data stored upon them or accessible by them, are well outside the universe of "closed containers" contemplated by the Supreme Court of yesteryear. Accordingly, a device's contents, including its cloud-accessible documents, must be stored until a warrant is obtained. Such an application would necessarily lead to a new understanding of technology's interplay with the Fourth Amendment. This understanding is crucial to the future of Fourth Amendment jurisprudence, given how strained technology privacy jurisprudence has become under the weight of obsolete analogies that ignore new technology's obvious, intrinsic qualities and instead classify it according to what James Madison was familiar with.