THE NEXT GENERATION COMMUNICATIONS PRIVACY ACT

Orin S. Kerr*

162 U. Pa. L. Rev. (forthcoming 2013).

Abstract

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to regulate government access to Internet communications and records. ECPA is widely seen as outdated, and ECPA reform is now on the Congressional agenda. At the same time, existing reform proposals retain the structure of the 1986 Act and merely tinker with a few small aspects of the statute. This Article offers a thought experiment about what might happen if Congress repealed ECPA and enacted a new privacy statute to replace it.

The new statute would look quite different from ECPA because overlooked changes in Internet technology have dramatically altered the assumptions on which the 1986 Act was based. ECPA was designed for a network world with high storage costs and only local network access. Its design reflects the privacy threats of such a network, including high privacy protection for real-time wiretapping, little protection for non-content records, and no attention to particularity or jurisdiction. Today's Internet reverses all of these assumptions. Storage costs have plummeted, leading to a reality of almost total storage. Even United States-based services now serve a predominantly foreign customer base. A new statute would need to account for these changes.

The Article contends that a next generation privacy act should contain four features. First, it should impose the same requirement on access to all contents. Second, it should impose particularity requirements on the scope of disclosed metadata. Third, it should impose minimization rules on all accessed content. And fourth, it should impose a two-part territoriality regime with a mandatory rule structure for United States-based users and a permissive regime for users located abroad.

---

* Fred C. Stevenson Research Professor, George Washington University Law School. This article was supported by the Daniel and Florence Guggenheim Foundation Program on Demography, Technology and Criminal Justice at the Law Library of Congress, where the author is presently serving as a Scholar in Residence. The author thanks Richard Salgado, Chris Soghoian, Al Gidari, Jim Dempsey, Marc Zwillinger, Chris Yoo, Eric Goldman, Edward Felten, Ryan Calo, Andrea Matwyshyn, Jerry Kang and Ramesh Ponnuru for helpful comments, as well as Cynthia Jordan, Robert Newlen, and David Mao at the Law Library of Congress for their support. This paper was also presented as the 2013 John Gedid Lecture at the Widener University Law School.

Table of Contents

Introduction

In 1986, Congress enacted a statute to govern the privacy of computer network communications known as the Electronic Communications Privacy Act (ECPA).[1] The Act grants Internet users a set of statutory privacy rights that limit the power of the government to access a person's communications and records.[2] ECPA has governed Internet privacy in the United States for over a quarter century with only minor changes.[3]

In recent years, it has become widely recognized that ECPA is outdated.[4] With the new Congress sworn in January 2013, ECPA reform has become a major issue on Capitol Hill. The Chairman of the Senate Judiciary Committee, Senator Patrick Leahy, recently announced that ECPA reform is now a "top priority."[5] His counterpart on the House side, Chairman Robert Goodlatte of the House Judiciary Committee, has also endorsed the need to reform ECPA and has recently held hearings on ECPA reform.[6]

---

[1] Pub. L. 99–508, 100 Stat. 1848 (October 21, 1986).

[2] *See generally* 2 WAYNE LAFAVE, ET. AL., CRIMINAL PROCEDURE 464-543 (3d ed. 2007).

[3] The major changes to ECPA following 1986 are discussed in Part IC, *infra*.

[4] *See* Charlie Savage, *Panel Approves a Bill to Safeguard E-Mail*, N.Y. TIMES, November 29, 2012, at B7 (noting that ECPA "is widely seen as outdated"); *see also* Brendan Sasso, *Consensus Builds for Requiring Warrant for Email Searches*, The Hill, March 19, 2013, http://thehill.com/blogs/hillicon-valley/technology/289035-consensus-builds-for-requiring-warrant-for-email-searches (quoting Rep. Jim Sensenbrenner as saying requirements of the ECPA are "outdated").

[5] Brendan Sasso and Jennifer Martinez, *House to Consider Email Privacy Bill*, The Hill, February 27, 2013, available at http://thehill.com/blogs/hillicon-valley/technology/285397-overnight-tech-house-to-consider-email-privacy-bill (describing ECPA reform as a "top priority" of Senator Leahy); *Leahy Lays Out Judiciary Committee Agenda For 113th Congress*, January 16, 2013, available at http://www.leahy.senate.gov/press/113-sjc-agenda-speech ("[A]s Chairman of the Judiciary Committee, I will keep pushing to update our privacy laws to address emerging technology and the Internet, including the Electronic Communications Privacy Act.").

[6] *See* Sasso & Martinez, *supra* note 3 (reporting the commitment of House Judiciary Chairman Robert Goodlatte to "look at modernizing the decades-old

Despite the Congressional interest in ECPA reform, existing reform proposals mostly nibble at the edges of the 1986 statute.[7] Those proposals accept the basic structure of ECPA as fixed, and they aim to tweak privacy protections within the 1986 framework. This Article considers a thought experiment: What would the electronic communications privacy laws ideally look like if Congress could start from scratch and enact an entirely new law?

The Article contends that such a new privacy act would look quite different from the current ECPA statute. Network technologies have undergone a dramatic transformation since the 1980s. The extraordinary pace of technological change in the last quarter-century means that the Internet of today bears only a slight resemblance to the Internet of the 1980s. Indeed, the Internet of today is quite different from the Internet of a decade ago, often in ways that are imperceptible to the user but have profound implications for privacy law. If Congress could start fresh and enact a new statute, those changes would lead to a law very different from the ECPA statute on the books today.

Two technological changes are particularly important. First, the plummeting costs of storage have flipped the default understanding of how surveillance threatens privacy.[8] ECPA was drafted at a time when electronic storage was expensive and therefore relatively rare. ECPA accordingly treated real-time wiretapping as the chief privacy threat. Access to stored communications was treated as a lesser concern. The opposite is true today. Storage has become remarkably cheap and therefore ubiquitous. Service providers now routinely store everything, and they can turn over everything to law enforcement. As a result of that technological change, access to stored records has become the greater privacy threat. The incredible growth of stored records makes ECPA's structure exactly backwards for the operation of modern computer networks.

The second technological change is that the Internet has become truly global.[9] ECPA was written at a time when computer network

---

Electronic Communications Privacy Act (ECPA) to reflect our current digital economy").

[7] *See* Part I.D, *infra*.

[8] *See* Part II.A., *infra*.

[9] *See* Part II.D., *infra*.

usage was very heavily based in the United States. The Act created statutory protections for United States users of United States services. Today's network usage looks dramatically different. Only about 10% of the today's global Internet usage involves individuals located in the United States.[10] The overwhelming majority of users of Internet services such as Gmail and Facebook are based abroad.[11] The global nature of today's Internet creates a series of jurisdictional headaches for global Internet services that might have corporate headquarters in one country, servers in another, and users all around the world.

More has changed than just technology: New principles of constitutional law have emerged that alter the proper role of statutory law. In the last five years, courts have begun to settle the basic parameters of how the Fourth Amendment applies to the Internet.[12] The original ECPA was designed as a statutory stand-in for uncertain Fourth Amendment protection. As the scope of Fourth Amendment protection becomes more certain, however, the required scope of the statute will necessarily change. Statutory protection originally designed to substitute for constitutional doctrine has become a hindrance thanks to limits on the exclusionary rule in when Congress provides statutory privacy rules.

As a practical matter, lawmakers rarely start from scratch in passing legislation. Amending prior laws is the norm for a range of reasons. But if Congress were forced to enact a new privacy act, that new law would be ideally based on four principles. *First*, the new statute should impose a uniform warrant requirement for compelled access to remotely-stored contents held for a customer or subscriber. The new statute should abolish the antiquated distinctions adopted by ECPA, such as the difference between real-time access and stored access and the complex categories of coverage of the Stored Communications Act. In place of those distinctions, the new statute should treat all access to contents under the same warrant standard.

Second, the law would enact a particularity requirement for compelled access to non-content information. One approach might rely on the concept of customer-hours. When the government obtains a

[10] *See id.*

[11] *See id.*

[12] Part II.C., *infra*.

court order to compel records, it should not be entitled to all records of a user – or even worse, all records of hundreds of users. Instead, each court order should be limited based on both the time coverage of the order and the number of users implicated. If the government wants records associated will many users, it should be forced to accept the tradeoff that those records span a shorter window of time.

Third, the new law would impose minimization limitations for contents of communications obtained by government investigators. When the government obtains the contents of communications pursuant to a court order, investigator should be limited in terms of what they can access. ECPA only imposed such limits for contents obtained by real-time wiretapping, reflecting the fact that real-time access posed a greater privacy threat at that time. The functional collapse of the distinction between real-time and stored access means that those limits should now apply to all contents.

Fourth, a new law would adopt an explicit territoriality regime. One solution would be to focus on the location of the user, with full warrant protections for users based on the United States and a permissive regime of disclosure to foreign legal process for users based abroad. A global network demands different protections for users based in the United States and users based abroad. United States users should receive full warrant protection regardless of the location of servers or corporate headquarters. On the other hand, United States providers should be permitted but not required to disclose records pursuant to foreign legal process for users based in the country seeking the records

The argument will proceed in three parts. Part I introduces the history and structure of ECPA. This section explores the computer technology that existed when ECPA was passed and explains how ECPA evolved in response to that technology. Part II explains why the existing statute is based on outdated assumptions. Changing technology and evolving constitutional law have dramatically shifted the factual and legal ground on which ECPA was enacted. Part III identifies the four major principles on which a next generation privacy act could be based. It points the way to new principles based on existing network technology.

I. The History and Structure of ECPA

It is difficult to analyze ECPA without first understanding early Internet technology and how ECPA was crafted in light of it. This section begins by explaining surveillance law before ECPA. It then turns to the new technological problems that ECPA was designed to address, and it next explains the basic structure of ECPA to see how it responded to the technology of that era. The section concludes by highlighting the limited nature of existing ECPA reform proposals by focusing on reforms advocated by an influential group known as the Digital Due Process Coalition.

(A) Federal Surveillance Law Before ECPA

Early federal surveillance laws began as efforts to regulate telephone privacy. The telephone was invented by 1880,[13] and it proved a dramatic advance over communication by telegraph. But the telephone had a serious privacy flaw. Any person who had access to the physical wires carrying the call could tap into the wire and intercept the call. In the early days of the telephone, wiretapping was rampant.[14] Some state laws prohibiting wiretapping emerged by 1895,[15] although the first federal statute did not arrive until the Communications Act of 1934.[16] Telephone privacy laws naturally focused on the act of intercepting the call – that is, breaking in on the private call and installing a listening device to monitor the communication over the wires as the call was transmitted.[17]

---

[13] Christopher Beauchamp, Who Invented the Telephone?: Lawyers, Patents, and the Judgments of History, 51 Tech. & Culture 854, 855-66 (2010).

[14] *See generally* SAMUAL DASH ET AL., THE EAVESDROPPERS (1959). *See also* Heutsche v. United States, 414 U.S. 898, 898-99 (1973) (Douglas, J., dissenting) (stating that "we live in a regime where the 'dirty business' of wiretapping runs rampant").

[15] *See* Berger v. New York, 388 U.S. 41, 46 (1967).

[16] *See* Pub. L. 416, Act of June 19, 1934, ch. 652, 48 Stat. 1064, codified at 47 U.S.C. 605 (1934).

[17] For example, the relevant provision of the Communications Act of 1934 stated that "[n]o person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person." 47 U.S.C. § 605 (1934).

Congress maintained the focus on interception when it enacted the Wiretap Act in 1968.[18] The Wiretap Act replaced the Communications Act of 1934 as the federal statute that governs privacy in telephone communications. Like the Communications Act, the Wiretap Act prohibits "intercepting" telephone calls between parties to a communication.[19] Unlike the Communications Act, however, the Wiretap Act includes a carefully crafted privacy regime regulating when interceptions were lawful.[20] That privacy regime was inspired in part by the Supreme Court's decision in *Berger v. New York*,[21] which required any wiretapping statute to include special privacy protections against government monitoring.[22] Wiretapping raises special Fourth Amendment concerns, *Berger* had indicated, because it involved "a series or a continuous surveillance" rather than the "one limited intrusion"[23] of a traditional search into physical property. Put another way, real-time wiretapping was contemporaneous with transmission and therefore could collect all information sent over the wire; in contrast, a traditional search was a limited intrusion into a space to collect only what had been stored there.

Echoing *Berger*, the Wiretap Act imposes an extra-high warrant requirement for intercepting telephone calls over the wires. Interception orders can be obtained to conduct government monitoring, but they require a showing of special need and a predicate felony offense as well as high-level Justice Department approval.[24] The Wiretap Act also includes two special rules for how the government must execute a wiretap. First, the government must engage in

---

[18] The Wiretap Act is sometimes called "Title III," as it was passed as the third title of the Omnibus Crime Control and Safe Streets Act of 1968, Pub.L. 90–351, 82 Stat. 197, enacted June 19, 1968. The Wiretap Act is codified at 18 U.S.C. §§ 2510-22.

[19] *See* 18 U.S.C. 2511(1)(a) (stating that anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" commits a crime).

[20] *See generally* 18 U.S.C. § 2511(2)-(3) (identifying exceptions when wiretapping is lawful without a court order); 18 U.S.C. § 2518 (identifying procedures for lawful interception pursuant to a court order).

[21] 388 U.S. 41(1967).

[22] *Id*. at 57-60.

[23] *See id*. at 57.

[24] *See generally* 18 U.S.C. § 2518.

minimization.[25] Minimization refers to the process of trying to limit ex ante which of a suspect's communications the government will intercept.[26] If an agent is listening to a wiretapped telephone line, the agent might engage in minimization by not listening in when the suspect speaks with his mother about her health problems.[27]

The second requirement is a general ban on disclosure of communications intercepted or information learned from those communications unless appropriate to the investigation.[28] Agents are not permitted to disclose what they learned from intercepted communications even to other agents unless it is "is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure."[29] The idea is to treat even lawfully intercepted communications as private: The government must justify each use and disclosure of information even within the government.[30]

(B) The OTA Report and the Need for ECPA

By the mid-1980s, Congress grew concerned about new computer telecommunications methods that were outside the scope of existing privacy laws. In 1985, the now-defunct Office of Technology Assessment published an influential report entitled *Electronic Surveillance and Civil Liberties*.[31] The report noted the growth of communications sent over computers, and specifically the advent of

---

[25] *See* 18 U.S.C. § 2518 (stating a wiretapping order "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception"); *see also* WAYNE LAFAVE, ET. AL., 2 CRIMINAL PROCEDURE § 4.6(h) (3d. Ed. 2007).

[26] *See* WAYNE LAFAVE, ET. AL., 2 CRIMINAL PROCEDURE § 4.6(h) (3d. Ed. 2007).

[27] *See* Scott v. United States, 436 U.S. 128, 142 (1978); United States v. Glover, 681 F.3d 411, 420-21 (D.C. Cir. 2012)

[28] *See* 18 U.S.C. §2517.

[29] 18 U.S.C. §2517(1).

[30] *See* SEC v. Rajaratnam, 622 F.3d 159, 175 (2d Cir. 2010).

[31] OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985) (hereinafter "OTA Report").The report is available online at http://www.fas.org/ota/reports/8509.pdf.

"electronic mail."[32] At that time, electronic mail took two forms. First, users could send messages that were then printed out and delivered in hard copy format either by the postal service or by a courier.[33] Second, users could send computer-to-computer messages over the telephone lines.[34] This generally required use of a modem to access mainframe computers, which would allow users to send their messages over the telephone lines where it would wait at a "central computer" for the recipient to access and download the message.[35]

Computer data transmissions and electronic mail raised several new problems not covered by the Wiretap Act. First, the Wiretap Act of 1968 was largely telephone-specific.[36] The interception of computer data transmissions was not prohibited by the Wiretap Act because the Wiretap Act only protected data transmissions that contained the sound of the human voice.[37] Data communications were excluded. This issue had arisen in the very first federal computer crime case when a hacker objected to being monitored using the network he had successfully invaded.[38] Such monitoring could not violate the Wiretap Act for several reasons, the Fourth Circuit held, among them because computer

---

[32] Notably, the privacy of e-mail dominated the Report's concerns about computer privacy. The report briefly noted that computer users also could access Electronic Bulletin Boards, but even these were described as a form of e-mail:

> An electronic bulletin board is an electronic mail service (or the equivalent computer-based information service) with a public or private electronic mailbox that is accessible to several persons. A public bulletin board usually is open to many or all subscribers and/or persons with a general password. A private bulletin board is limited to persons with special passwords."

See id. at 48.

[33] *Id*. at 48.

[34] OTA Report at 47.

[35] *Id*. at 48.

[36] The Wiretap Act also prohibits the interception of "oral communications," which effectively prohibits the use of secret audio recording devices record the human voice. *See* 18 U.S.C § 2511(1)(a); 18 U.S.C. § 2510(2) (defining "oral communication"). The oral communication aspects of the Wiretap Act are not implicated by the issues raised in this article.

[37] See OTA Report at 36.

[38] *See* United States v. Seidlitz, 589 F.2d 152, 156-57 (4th Cir. 1978).

transmissions did not contain sounds and therefore were not protected by statutory law.[39]

Second, the Wiretap Act only applied to real-time interception instead of access to stored communications.[40] This made sense with ephemeral telephone calls. The only way to access a phone call was to listen in real time as the call occurred. But electronic mail was stored at various places in the course of delivery, and accessing a stored communication was not an "interception" because it was not contemporaneous with its transmission.[41] As a result, the Wiretap Act did not offer any protection against government access to stored e-mail.[42] The Fourth Amendment might protect individuals against government access to their stored e-mails, the OTA Report noted.[43] But the possible scope of Fourth Amendment protection was uncertain, and any protection might not apply to backup copies held by "electronic mail companies"[44] that the government could access.

(C) The Enactment of ECPA, and Its Major Amendments

In 1986, just a year after the OTA Report, Congress enacted ECPA to provide for privacy protections in the new uses of computer technologies.[45] ECPA consisted of three parts. The first part expands the Wiretap Act so that its prohibition on interception extended to computer data transmissions in addition to telephone calls.[46] Another part of the statute adds protections against the use of pen registers, which were tools used to monitor the numbers dialed from a person's telephone.[47] Sometimes known as the Pen Register Statute, this portion of ECPA makes it unlawful to install a monitoring device to record telephone numbers unless the government first obtained a court order

---

[39] *See id.* at 157.

[40] At the time, the leading precedent on this point was United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976)

[41] *See id.*.

[42] *See* OTA Report at 48-50.

[43] *See id.* at 50.

[44] *See id.*

[45] *See* Pub. L. 99–508, 100 Stat. 1848 (October 21, 1986).

[46] This amendment was Title I of ECPA, and it amended 18 U.S.C. §§ 2510-22.

[47] This amendment was Title III of ECPA, and it was codified at 18 U.S.C. §§ 3121-27.

or else the phone company recorded the numbers for its business purposes.[48]

But the most complex part of the new statute, and the part that has become by far the most important, is a provision that has come to be known as the Stored Communications Act (SCA).[49] The SCA creates statutory privacy rights for "subscribers or customers" of two kinds of Internet services.[50] The first kind of Internet service protected by the statute is the one most relevant to individual users. The statute creates privacy protections in e-mail services, referred to in the statute as "electronic communications service" providers ("ECS").[51] The second kind of Internet service protected by the statute was (at least at the time) of primary interest to businesses. Businesses such as hospitals and banks often outsourced storage and processing services to commercial services.[52] This was true because computer storage was very expensive, and business software such as spreadsheet programs had not been invented. Congress opted to create statutory privacy protections for the customers of these commercial services, referred to in the statute as providers of "remote computing services" ("RCS").[53]

The statute then creates two kinds of protections for customers of the two covered providers. First, it creates legal rules on when the government could compel the providers to disclose records about customers and subscribers; and second, it created legal rules on when the providers could disclose records voluntarily.[54] Significantly, the rules for both compelling and voluntarily disclosing records act as an on/off switch: Where *any* category of records can be disclosed, *all* records held by the provider can be disclosed. To put the point in language from the Fourth Amendment context, the statute imposes no

---

[48] *See* 18 U.S.C. § 3121. For a helpful discussion of the Pen Register Statute, *see* In re Application of the United States of America, 846 F.Supp. 1555 (M.D. Fla. 1994).

[49] The Stored Communications Act was enacted as Title II of ECPA, and it is codified at 18 U.S.C. §§ 2701-11.

[50] *See* 18 U.S.C. § 2702.

[51] *See id*.

[52] S. Rep. NO. 99-541 (1986), at 10-11.

[53] *See id.*

[54] In the current version of the statute, the rules on compelled disclosure are found in 18 U.S.C. § 2703 while the rules on voluntarily disclosure are found in 18 U.S.C. §§2702.

limits on particularity: There is no need to be specific as to which e-mails, which files, or which records were obtained. Instead, disclosure of one record allows disclosure of all records.

Unlike the Wiretap Act of 1968, the SCA of 1986 is notable for imposing no minimization requirement. Under the Wiretap Act, lawful access to communications comes with strings attached. Even after obtaining a lawful wiretap order, agents are required to screen communications ex ante. No such limitations were imposed under the SCA. Under the SCA, a court order requires the provider to provide the government with the entire contents of the account. The government is then free to look through all of it, and the SCA imposes no limits on the government's power to use communications it finds whether relevant or not to the crime under investigation.

In any communications network, a fundamental distinction exists between the actual message to be sent over the network and information on the network that relates to the how, when, and where of the message. The former is the content of the communication; the latter, non-content records sometimes known as meta-data or envelope information.[55] In the context of Internet communications, the contents include the actual messages in e-mails, together with their subject lines, as well as the contents of files stored on the network.[56] In contrast, the meta-data includes IP addresses, to/from information on e-mails, login times, and locations.[57] As enacted in its original form, the SCA focused its attention on contents held by providers of ECS and RCS instead of non-content information. Unopened e-mails stored for less than 180 days received the full protection of a warrant. [58] Opened e-mails and remotely stored files held by providers of RCS received less protection.[59] But protections for non-content information were the weakest protections in the statute and appear to be added almost as an afterthought.[60]

---

[55] For postal letters, the difference is the letter versus the outside of the envelope.

[56] *See generally* Orin Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 611-13 (2003).

[57] *See id*.

[58] *See* 18 U.S.C. § 2703(a).

[59] *See* 18 U.S.C. § 2703(b).

[60] *See* 18 U.S.C. § 2703(c) (1986).

Although the basic structure of the 1986 statute remains in place today, two subsequent amendments are worth noting. First, in 1994, Congress bolstered the privacy protections for some kinds of non-content information.[61] Under the 1994 amendment, the government must establish specific and articulable facts to obtain a court order requiring the disclosure of many kinds of non-content Internet records, such as the to/from addresses on e-mails.[62] This is the reasonable suspicion threshold familiar to students of Fourth Amendment law.[63] Congress codified the section that provides for this order at 18 U.S.C. 2703(d), and as a result the court orders are known colloquially as "2703(d) orders."[64]

Second, as part of the Patriot Act in 2001, Congress amended the pen register provisions of ECPA to clarify that they apply to Internet communications as well as telephone calls.[65] The 1986 text of the pen register provisions of ECPA was largely telephone-specific.[66] It prohibited the installation of devices to record telephone numbers dialed absent a court order.[67] At the same time, the 1986 text left unclear whether the statute only provided privacy protections for numbers dialed in telephone calls or if they also applied to the real-time acquisition of non-content records relating to Internet communications.[68] The Patriot Act clarified that the pen register sections of ECPA apply to the Internet by redefining terms such as "pen register" to include all "dialing, routing, addressing, and signaling

---

[61] *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414 (1994) at § 207(2).

[62] *See id.*

[63] *See* United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) (stating that "the 'specific and articulable facts' standard [in 18 U.S.C. § 2703(d)] derives from the Supreme Court's decision in *Terry*.")

[64] *See* LAFAVE, *supra* note 2, at § 4.8(c) ("The court order found in § 2703(d) is often referred to as a '2703(d)' order or simply a 'd' order.").

[65] *See* Kerr, *supra* note [], at 623-43.

[66] *See id.* at 633-36.

[67] From 1986 to 2001, a pen register was defined by the statute as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3) (1986).

[68] *See* Kerr, *supra* note [], at 633-36.

information" relating to any telecommunications network.[69] As a result, the pen register provisions of ECPA now extend to government surveillance of non-content addressing information such as Internet Protocol addresses and the to/from information for e-mail communications.

The ECPA that emerges from the original 1986 statute and its major amendments is premised on a series of dichotomies. Knowing how the statute regulates a particular kind of privacy-invading action requires classifying the act based on the statute's major criteria. For example, is the surveillance occurring in real time (prospectively), or does it involve access to stored records (retrospectively)? The Wiretap Act and Pen Register provisions of ECPA apply in the former case; the Stored Communications Act provisions apply in the latter case. Does the conduct involve access to contents of communications, or does it involve access to non-content envelope information? The former are regulated by the Wiretap Act and parts of the Stored Communications Act, while the latter are regulated by the Pen Register provisions and different parts of the Stored Communications Act. Are the communications held by a remote computing service or electronic communications service? Is the disclosure voluntary or compelled? Again, the answer points the reader to a different section of the statute with different protections.

(D) The Current Criticisms of ECPA – And Their Limits

ECPA was an impressive achievement in its day. A quarter century later, however, it has become commonplace to recognize that ECPA is outdated.[70] But although the need to update ECPA is widely recognized, existing criticisms of the statute and current reform proposals merely tinker around the edges of the statute. The proposals retain the basic structure of the statute and only "update" a few isolated aspects of its overall structure.

---

[69] 18 U.S.C. § 3127(3).

[70] *See* Charlie Savage, *Panel Approves a Bill to Safeguard E-Mail*, New York Times, November 29, 2012, at B7, available at http://www.nytimes.com/2012/11/30/technology/senate-committee-approves-stricter-privacy-for-e-mail.html (noting that ECPA "is widely seen as outdated").

Perhaps the best way to appreciate the limited nature of existing criticism is to appreciate the reform proposals recently advocated by a large and influential set of civil liberties groups, Internet companies, and privacy scholars known as the Digital Due Process Coalition.[71] The group includes non-profit organizations such as the American Civil Liberties Union and the Electronic Frontier Foundation as well as major Internet businesses including Google, Apple, Facebook, Amazon, Microsoft, and AT&T.[72] Understanding the Coalition's four principles provides a helpful illustration of the limited ambitions of existing ECPA reform proposals.

The first proposal of the Digital Due Process Coalition would impose a warrant requirement for compelled government access to stored contents of communications held by a provider of ECS or RCS.[73] Some background may be helpful to understand this proposal. The SCA imposes a warrant requirement in some cases but not others. On one hand, the government needs a warrant to compel the contents of communications held by a provider of ECS for up to 180 days.[74] On the other hand, the government does not need a warrant to compel the contents held by a provider of ECS for more than 180 days or held by a provider of RCS.[75]

Under this framework, the SCA offers less protection than a warrant to regulate government access to many remotely-stored personal files. For example, old e-mails are no longer fully protected

---

[71] The corporate members of the group include a virtual "who's who" of the Internet world. *See generally Who We Are*, http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163.

[72] The group maintains a website at http://digitaldueprocess.org/

[73] "A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations." available at http://digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

[74] 18 U.S.C. § 2703(a).

[75] 18 U.S.C. § 2703(b).

under the ECS rules.[76] Also, because individuals often use third party Internet storage services that count under the RCS rules – think of Google Docs[77] and other cloud storage services – many of their personal files are protected by less process than a warrant under the RCS rules, as well. The first proposal of the Digital Due Process Coalition would replace that patchwork of protections with a simple warrant requirement for all contents held by a provider of RCS or ECS for any length of time.

The second Coalition proposal would require a warrant whenever the government compels ECS or RCS providers to disclose location information for mobile devices such as cell phones.[78] Mobile devices create location records because device providers need to know where the devices are located to route communications to and from them. Cellular phones did exist when ECPA was first drafted, although the statute did not provide for any special rules to govern access to records relating to their use. Instead, the current statute treats mobile location information like other non-content records. Under the Stored Communications Act, retrospective government access to stored location information generally requires a 2703(d) order.[79] On the other hand, because ECPA does not provide for prospective access to location information,[80] the government generally must obtain a warrant under

---

[76] This may be true for two reasons. First, the e-mail may be in electronic storage for more than 180 days, and thus may be covered under 18 U.S.C. 2703(b). Alternatively, some courts have held that opened e-mail that is stored on a server is held in the provider's capacity as a remote computing service, and thus becomes covered under § 2703(b) immediately after it is opened and the copy is stored. *See* Jennings v. Jennings, 736 S.E.2d 242 (S.C. 2012). But see

[77] *See generally* docs.google.com (last visited March 6, 2013).

[78] *See* DDPC Proposal, *supra*. ("A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.").

[79] *See* 18 U.S.C. § 2703(c).

[80] The Pen Register statute might be thought to regulate prospective access to location information, but Congress indicated a contrary intent in a section of the Communications Assistance to Law Enforcement Act. *See* 47 U.S.C. § 1002(a)(2)(B) "("[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber").

the Federal Rules of Criminal Procedure to obtain ongoing access in "real time" to such location information.[81] The coalition proposal would extend the statutory warrant requirement to retrospective collection of stored location information.

The third Coalition proposal is to raise the statutory threshold for pen register information.[82] Under the pen register provisions of ECPA, the government can obtain an order to collect non-content addressing information in real-time with a mere certification that the information to be collected is believed to be relevant to an ongoing investigation.[83] No showing of reasonable suspicion or probable cause is required, and the judge does not make an independent determination of the facts. The coalition proposal would require the government "at least" to satisfy the reasonable suspicion standard of a 2703(d) order.

The final Coalition proposal would limit the government's power to subpoena account information for multiple individuals or accounts.[84] ECPA permits the government to compel a limited set of information about accounts with a mere subpoena, such as a subscriber's name and address (if known); records of session times and durations; and IP addresses.[85] The coalition would maintain this power but clarify that multiple subpoenas are needed for multiple accounts unless the government establishes some sort of cause for multi-account orders.

The four proposals of the Digital Due Process coalition provide a helpful sense of the kinds of ECPA reform proposals that have been made in recent years, both in the academic scholarship and in

---

[81] Lower courts are not uniform on this point, but it is the majority view and in my view correct. S*ee generally* In re Application of U.S. for and Order Authorizing Disclosure of Location–Based Servs., 727 F.Supp.2d 571 (W.D.Tex. 2010).

[82] *See* DDPC Proposal, *supra*. ("A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).")

[83] See 18 U.S.C. § 3122.

[84] *See* DDPC Proposal, *supra*. ("Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.").

[85] 18 U.S.C. § 2703(C)(2).

Congressional bills. But it is striking how much the proposals accept the basic structure of the 1986 statute. They accept the existing coverage of the Wiretap Act, Stored Communications Act, and Pen Register statute. They accept the existing distinction between real-time and stored access; the distinction between content and non-content; and the existing definition of ECS and RCS. Three of the four proposals focus on a single narrow question: the thresholds of cause that the government must satisfy to compel information from a provider in various contexts.

To be clear, I agree with some of the Coalition's proposals.[86] But whether one agrees or disagrees with them, the existing proposals do not so much update ECPA as they increase privacy protections using the ECPA's outdated framework. The remainder of this article takes a different approach. Instead of asking how existing laws might be tinkered, it considers what law Congress should enact if it were to enact new privacy laws from scratch. Internet technology and Fourth Amendment law is far from where they were in the 1980s, and those changes indicate that starting from scratch would bring Congress to enact a very different statute. The next section shows why.

II. How Changing Law and Technology Render ECPA Obsolete

This section explains how current technology and constitutional law have rendered the dichotomies of ECPA obsolete. ECPA is premised on a series of dichotomies created by the original 1986 Act. Several of the dichotomies are explicit, including real-time access versus stored access, ECS versus RCS, and content versus non-content. Others are implicit in the statute, such as the territorial scope of the statute and the

[86] For example, I advocated the coalition's third proposal in a 2003 article. *See* Kerr, *supra* note [], at 643 ("I agree with civil libertarian critics who believe that the pen register standard should be raised."). I have also testified about the Digital Due Process Coalition principles before the House Judiciary Committee. *See Testimony of Orin S. Kerr, Hearing on Electronic Communications Privacy Act Reform, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, House Judiciary Committee*, May 5, 2010, available at http://judiciary.house.gov/hearings/pdf/Kerr100505.pdf

particularity of court orders. ECPA's distinctions made sense in a world in which few records were created, few records were stored, and therefore few records could be obtained. The statutory structure presumes an absence of Fourth Amendment protection, and it also presumes a world of users, providers, and users all inside the United States.

Today's network is very different. We have entered a world of almost total storage, in which providers and many users can and often do store everything. The Internet has become truly global, with many prominent United States based Internet services serving a predominantly foreign customer base. And Fourth Amendment protections are becoming established in ways that may soon outpace statutory standards. The old categories no longer work, indicating a need for new categories that should form the basis of a next generation privacy act. This section explains how the major distinctions of ECPA have become obsolete. It shines a light on the network technology of the present, revealing some surprising ways that the existing ECPA statute has become badly outdated.

(A) Real-time Versus Stored Access

The first fundamental dichotomy in ECPA is the distinction between real-time surveillance and access to stored records. Real-time surveillance is covered by the Wiretap Act and Pen Register statute; access to stored records is covered by the Stored Communications Act. The statutory distinction between prospective and retrospective surveillance emerged for largely historical reasons. The telephone network predated the Internet, and telephone surveillance was necessarily real-time. Also, the Supreme Court in *Berger v. New York* indicated that real-time wiretapping raised special privacy concerns: "continuous surveillance" raised the prospect that the government would need to monitor a great deal of unrelated private communications over time in order to find the small subset of communications related to criminal activity.[87] In contrast, access to stored communications raised much less of a concern, as relatively few communications were retained and therefore stored. As a result, real-time wiretapping required more privacy protections that stored access.

[87] *See* Berger v. New York, 388 U.S. 41, 59 (1967).

That distinction made sense when Congress enacted ECPA. In the 1980s, remote computer storage was very expensive.[88] Internet services of that time were designed to limit storage. After a user read his e-mail from a server, for example, the e-mail typically was downloaded to the user's computer and deleted from the server to save space.[89] Back when remote storage was expensive, the difference between real-time and stored access was important. Only very few communications that were sent were actually saved: Real-time access raised special concerns that stored access did not. For that reason, Congress created special restrictions such as minimization on real-time data collection. The government had to carefully limit what information it accessed and then limit what it disclosed. No similar protections were written into the Stored Communications Act.

Today, however, the distinction between stored and real-time surveillance has blurred. Storage has become extremely cheap. Computer storage costs have dropped by a factor of 10 roughly every 4 years for the last 30 years.[90] The cost of storing a single gigabyte of data has dropped from about $85,000 in 1984 to about five cents in 2011.[91] As the cost of storage drops, Internet services offer the capacity to store everything cheaply. Massive amounts of storage have become the norm. And as massive storage becomes so cheap that it is virtually free, the norm among users changes along with it. Users no longer need to be careful about what they keep on the server. The server can keep everything.

To appreciate the difference, consider the storage space available to users of free web-based e-mail services. When free e-mail services became popular in the mid to late 1990s, they generally came

---

[88] For an examination of the evolution of data storage systems and their costs, see R. J. T. Morris & B. J. Truskowsi, The Evolution of Storage Systems, 42 IBM Sys. J. 205 (2003).

[89] *See* OTA Report, *supra*.

[90] John Villasenor, R*ecording Everything: Digital Storage as an Enabler of Authoritarian Governments*, Brookings Institution, available at http://www.brookings.edu/~/media/research/files/papers/2011/12/14%20digital%20storage%20villasenor/1214_digital_storage_villasenor.pdf

[91] *See id.*; *see also* Morris & Truskowsi, supra note 88 (noting that since 1997 raw storage prices have been declining at 50-60% per year).

with about 2 megabytes of storage space.[92] In contrast, today's popular free gmail service comes with 15 *gigabytes* of storage space, about 7,500 times more storage than was common a decade ago.[93] And it is taken for granted that the space that comes with free e-mail services will only continue to increase.[94]

Many readers will appreciate how the difference has changed their approach to e-mail storage. A decade ago, it was commonplace for users to delete many stored communications to save space. Today the norm has flipped. The commonplace reaction is to store everything and simply search through data later to find what the user needs. The statistics bear this out. According to one recent report, a typical gmail user stores more than 17,000 e-mails in her account at any given time.[95] Almost 12,000 of those e-mails are received e-mails stored in the inbox; Almost 6,000 are sent e-mails directed elsewhere.[96]

The drop in storage costs has led to a shift in the practices of Internet providers. Today's Internet providers can and often do store everything. The Boston Police Department revealed a fascinating example in 2009 when it released documents investigators had collected pursuant to ECPA to solve the case of the so-called "Craigslist Killer," Philip Markoff.[97] Among the documents was a report the police

---

[92] *See* Paul Festa, *Google to Offer Gigabyte of Free E-mail*, CNET News, April 1, 2004, available at http://news.cnet.com/2100-1032-5182805.html

[93] See Nathan Ingraham, *Google Unifies Gmail, Drive, And Photo Storage: All Users Now Get 15GB Of Shared Space*, The Verge, May 13, 2013, available at http://www.theverge.com/2013/5/13/4326994/google-unifies-gmail-photo-and-drive-storage.

[94] Indeed, the amount of space provided to Gmail users rose from 10GB to 15GB in between drafts of this article. *See* Chris Ziegler, *Gmail Bumps Free Storage to 10GB*, *The Verge*, April 24, 2012, available at http://www.theverge.com/2012/4/24/2971885/gmail-bumps-free-storage-to-10gb.*See id.* (reporting on the increase to 10GB and predicting that, "as always," the amount of free storage will continue to "creep up over time").

[95] *See* Mike Barton, *How Much Is Your Gmail Account Worth?*, Wired, available at http://www.wired.com/insights/2012/07/gmail-account-worth/

[96] *See id.*

[97] *See* Carly Carioli, *When the Cops Subpoena Your Facebook Information, Here's What Facebook Sends the Cops*, The Phoenix, http://blog.thephoenix.com/blogs/phlog/archive/2012/04/06/when-police-subpoena-your-facebook-information-heres-what-facebook-sends-cops.aspx

had obtained from Facebook containing the stored contents of Markoff's Facebook account. The 72-page report contained more than just all of the messages, friends list, and pictures that we might think of as the contents of a Facebook account.[98] It also contained every comment Markoff had posted and all of the deleted pictures and deleted friends he had once had but then tried to erase. And more remarkably, it also contained records of *every single click* that Markoff had made while using Facebook. Every visit to every page, every viewing of every picture, and every click on every link was documented with a specific entry in a log file.[99] Facebook had recorded it all.

As these examples suggest, the drop in the price of storage has caused an unappreciated sea change in the practical implication of access to stored communications. The default has switched from store-only-important-records to store-it-all. Granted, Facebook does not store everything only because it is cheap. Facebook's business model depends on being able to sell targeted advertisements based on what users do, which requires close monitoring of what they do.[100] But the low cost of storage makes that possible.

The change has enormous implications for Internet surveillance law. When everything is stored, stored access begins to reveal the same level of detail as real-time access. The difference between real-time surveillance and stored access evaporates. If anything, stored access becomes even more revealing and invasive than access in real time. Real-time surveillance is cabined by time. For example, thirty days of real-time surveillance can only reveal communications over the thirty-day period. In contrast, a single access to stored contents can reveal the complete details of communications *over a period of years*. The ability to store everything makes storage the greater privacy threat. Real-time surveillance becomes only a slice of the world that access to stored contents can produce.

The surprising rarity of investigative real-time wiretapping for Internet communications helps confirm the point. Federal law requires

---

[98] The contents have been posted online and are available at http://www.scribd.com/fullscreen/88465177?access_key=key-247mvzrfrh1m1azdsoai

[99] *See id.*

[100]

the Administrative Office of the U.S. Courts to publish an annual wiretapping report that discloses the number and type of wiretapping orders obtained pursuant to state and federal wiretap statutes.[101] In 2011, the most recent year available, a total of 2,092 wiretap orders were obtained to intercept telephone communications.[102] But here's a puzzle: Astonishingly few wiretap orders were obtained for Internet communications. The total number of federal wiretaps obtained to intercept "electronic communications" – that is, Internet and computer communications – was one.[103] That's not a typo. In the entire United States, federal investigators obtained a single Title III order to obtain Internet communications.[104] The same report discloses that state investigators acting pursuant to state wiretap acts obtained another three orders to collect Internet communications.[105] In a country of more than 300 million people, federal and state investigators obtained a total of four reported computer-specific wiretaps in 2011.[106]

This does not mean that investigators took a holiday from collecting evidence over the Internet. Instead, investigators have focused their attention on collecting stored records. Recent Google Transparency Reports provide some useful data. In the last six months of 2012, state and federal investigators in the United States obtained 1,896 search warrants for accounts operated by Google (most of which were for the contents of gmail accounts).[107] In light of current trends,

---

[101] The most recent report is documents orders during the year 2011. It is available at http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/2011WireTap.pdf

[102] *See* 2011 Wiretap Report, Table 6, Types of Surveillance Used, Arrests, and Convictions for Intercepts Installed January 1 Through December 31, 2011 http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table6.pdf

[103] *See id.*

[104] Another eight federal orders were obtained for orders that included some combination of telephone surveillance, Internet surveillance, and physical bugging, although the report does not disclose how many of those included Internet surveillance. *See id.*

[105] *See id.*

[106] It is fair to wonder if the reported number of state wiretap orders is valid, as state reporting practices may vary considerably. The reported number of federal wiretaps is very likely accurate because all Wiretap Act applications at the federal level must go through the Justice Department's Office of Enforcement Operations.

[107] http://www.google.com/transparencyreport/userdatarequests/US/

this would mean that Google likely received about 4,000 warrants for the contents of accounts in the year 2012. And of course Google is only one provider among many. Only a small percentage of e-mail accounts in the United States are hosted by Google. If the number of warrants executed at Google are representative, federal and state agents probably execute in the neighborhood of 20,000 to 30,000 search warrants for stored e-mail contents per year.

To be sure, the changing costs of storage are not the only explanation for this shift in practices. The increased use of encryption has made real-time Internet wiretapping much more difficult than it was previously. Because services tend to store the contents of communications in plaintext even if they send communications in ciphertext, the government naturally will try to collect the communications when they are stored rather than in transit.[108] Also, the investigative focus on stored communications partially reflects the lower statutory threshold for access to stored communications. A standard search warrant is sufficient to compel a provider to disclose stored contents, while real time surveillance requires a Title III "super warrant" that is substantially harder to obtain.[109] But the difference also reflects the reality that stored access is a more than adequate substitute in most investigations. The low cost of storage ensures that stored access and real-time surveillance generally produce the same level of detail. Technological change has reversed the assumptions of the 1986 statute.

(B) ECS vs. RCS, and the Limited Coverage of the SCA

The second fundamental dichotomy in ECPA is the distinction between providers of electronic communication service and remote computing service. In 1986, this reflected the two primary ways that users stored files on computer networks.[110] The ECS protections covered e-mail; the RCS protections covered contents of communications transmitted for remote storage and processing by

---

[108] See Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871.

[109] *See id.* (indicating the trend of increasing numbers over time).

[110] *See* Part I.B, *supra*.

services available to the public. The SCA does not protect any other kinds of contents because they fall out of the two kinds of network services that were common in 1986.

This approach is obsolete today for two reasons. First, it likely leaves unprotected perhaps the most private kinds of communications sent by modern Internet users: Search requests. Search engines did not exist in 1986 because the World Wide Web had not yet been invented.[111] There was no Web to search. Today, however, we send our most private thoughts to Google and other search engines to explore our questions, hopes, fears, fantasies, and dreams. According to one study, search engines analyzed about 18.4 billion search requests from the United States in the month of March 2012 alone.[112] That's about two searches a day per person in the United States, or more than 650 searches per year. Search engines store all of those requests, often for months or even years. For example, Google presently stores search queries for 18 months, and previously had stored them indefinitely.[113]

ECPA likely offers no protection for access to stored search queries, however, because it does not fit the 1986 dichotomies that the statute codifies. Search engines plainly do not provide ECS. They are destinations for communications, not providers of connectivity or messaging.[114] And search queries appear not to be protected under the RCS protections, either. A remote computing service is defined as a service that provides the public "computer storage or processing

---

[111] The Web was first invented in 1990, and the first browser was introduced in 1994. *See* Tim Berners-Lee With Mark Fischetti, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web 69 (1999); Nicholas Carr, The Big Switch: Rewiring the World, From Edison to Google 17 (2008).

[112] *See* Press Release, *comScore Releases March 2012 U.S. Search Engine Rankings*, http://www.comscore.com/Insights/Press_Releases/2012/4/comScore_Releases_March_2012_U.S._Search_Engine_Rankings

[113] Thomas Crampton, *Google To Cut Back On How Long It Keeps Search History*, June 12, 2007, available at http://www.nytimes.com/2007/06/12/business/worldbusiness/12iht-google.4.6113031.html?_r=0

[114] 18 U.S.C. § 2510(15) defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications." This limits ECS providers to providers of connectivity or messaging of covered wire or electronic communications.

services by means of an electronic communications system."[115] Users do not send their search queries to Google in order for Google to store them. Storage is a bug for users, not a feature.

Whether ECPA protects search queries therefore hinges on whether search engines "process" data that users send to them. The relevant text and legislative history suggests that they do not. In the context of computer data, the word "process" suggests operations on that data not in response to a query. The legislative history makes the context clear: remote processing meant the outsourcing of tasks, such as number-crunching, that a computer of the 1980s might not be able to complete easily.[116] Search engines don't seem to fit the mold. Users do not use search engines as substitutes for the storage or processing powers of their own machines. Although the issue is not crystal clear, [117] it appears likely that the most private of today's communications likely receive no statutory protection from ECPA.

---

[115] 18 U.S.C. § 2711(2).

[116] The Senate Report accompanying the passage of ECPA offered the following explanation of the concept of a "remote computing service" :

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse 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. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer.

S. Rep. No. 99-541 (1986), at 10-11.

[117] At least one major search engine, Google, claims to be covered by the SCA on the ground that it provides RCS. In litigation over the disclosure of Google search queries, Google made the following argument that its services are protected by the SCA:

> Google processes search requests as directed by, and for, its users who in turn retrieve the search results of their choosing from Google's index, or Google sends the results by email or text messages to individuals, to wireless phones or other designated mobile devices. Said in plain language, users rely on the

A second problem with the ECS/RCS dichotomy is that Internet services today are routinely multi-functional. In 1986, users accessed the Internet by connecting to mainframe computers.[118] Those mainframe computers gave users access to the network and an e-mail account. In the language of ECPA, they were ECS providers that gave users access to services including RCS providers. Today, however, users connect to the Internet in many different ways, including through broadband and wireless accounts. Network access is always on and running in the background rather than a conscious user destination.[119] At the same time, content messaging such as e-mail or text messages is simply one service available among many bundled together. Take the example of Facebook.[120] Facebook is not just an e-mail service. Rather, Facebook offers an amalgam of many different kinds of services, including e-mail, chat rooms, photograph hosting, search functions, and bulletin board services.

The multi-functional nature of modern Internet services creates headaches for ECPA by creating complex and perhaps unanswerable questions of what the statute protects. ECPA privacy protections hinge on the status of the provider. Given that providers wear multiple hats, the privacy protections that apply to records can have multiple answers. Imagine that a provider provide acts as an ECS for some communications, an RCS for others, and neither an ECS nor an ECS for a third. What privacy protections should apply when the government seeks the disclosure of records under the statute? If the government is seeking non-content records, the current statute offers conflicting answers to what privacy protection should apply depending on what service you imagine the provider to provide as it related to those

---

> remote computer facilities of Google to process and store their search requests and to retrieve by electronic transmission their search results.

See Google's Opposition to the Government's Motion to Compel in Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006), available at 2006 WL 543697.

[118] It was also during this time that personal computers began to make gains on the mainframe-computing model. *See* Carr, *supra* note 111, at 54-55.

[119] *See* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss. L.J. 1309, 1314 (2012).

[120] *See* facebook.com -- as if any cite were necessary.

records.[121] The old dichotomies do not fit today's technological practices.

(c) Content Versus Non-Content Metadata

The next dichotomy in ECPA is the distinction between the contents of communications and non-content metadata. When ECPA was first enacted, the statute focused on providing statutory protections for contents. The scope of Fourth Amendment protection for such contents was unclear.[122] Statutory protection provided privacy if the Fourth Amendment protections did not materialize or at least until they did so. In contrast, ECPA protections for non-content information were an afterthought.[123] Although later amendments paid more attention to privacy concerns in non-content records, the statute maintains its focus on protecting contents.

Such a focus may no longer make sense for two complementary reasons. First, changing technology has rendered metadata analysis more important. The capacity of computers to efficiently analyze metadata has made metadata surveillance more significant than it was in the past. The line between contents and metadata remains

---

[121] For example, imagine a company employee logs in to the company server to write an e-mail and view a stored document. The government wants records from the company about the employee's conduct. If the government is seeking those records from the company in its capacity as an e-mail provider – that is, as a provider of ECS -- then it needs a 2703(d) order to compel the non-content records. But if the government is seeking those same records from the company in its capacity as a private company that has log-in records about accessing the stored file, then ECPA doesn't apply at all: The provider is not an ECS because it is not providing e-mail service with respect to that file and cannot be a provider of RCS because it is not available to the public. Whether the statute applies depends on the metaphysical question of whether you see the records as related to the e-mail or the stored file.

[122] *See* OTA Report, *supra* note []. The only significant decision applying the Fourth Amendment to computer networks before the late 1990s was United States v. Horowitz, 806 F.2d 1222 (4th Cir. 1986), which was handed down a few months after ECPA passed. Further, Horowitz was more interesting for the issues it raised than the issues it answered. The defendant had sent information electronically to a customer, and the government recovered the information from the customer's server. *Id*. at 1224. The Fourth Circuit had no problem concluding that the defendant did not have Fourth Amendment rights in the data he had sent to the customer and that was available on the customer's computer. *See id.* at 1225-26.

[123] *See* Part I.C., supra.

fundamental,[124] but metadata analysis has become a more powerful tool than in the past. Metadata analysis has also become comparatively important with the rise of encryption.[125] Internet services that generate metadata possess it in unencrypted form. Encryption that might complicate or entirely thwart content surveillance may leave metadata available for government analysis.[126]

Second, changing law may be rendering the content protections of ECPA much less important. In the last few years, a number of lower courts have ruled that the Fourth Amendment fully protects the contents of e-mails held by third party providers. The leading case is *United States v. Warshak*,[127] a Sixth Circuit decision by Judge Boggs involving government access to e-mails held by Yahoo!. Investigators relied on the provision of the SCA allowing the government to obtain contents with less process than a warrant to subpoena Yahoo! for the contents of stored e-mails relating to a massive fraud scheme.[128] Yahoo! complied, and it gave investigators copies of thousands of e-mail messages without a warrant. The Sixth Circuit held that obtaining the contents of e-mails without a warrant was unconstitutional: Users have a reasonable expectation of privacy in their e-mails just like their letters and phone calls.[129] As a result, the provision of the SCA permitting the government to obtain e-mails with less process than a warrant was unconstitutional.[130]

Several courts have agreed with the Sixth Circuit since *Warshak*, including federal courts in Kansas[131] and the District of Columbia,[132]

---

[124] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1019-22, 1034-35 (2010).

[125] *See generally* Swire, *supra* note 108.

[126] I use the term "may" because the details depend on complex questions of what is defined as contents and what is defined as metadata. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 646, 646 n. 190 (2003).

[127] 631 F.3d 266 (6th Cir. 2010).

[128] *See id.* at 282-83.

[129] *See id.* at 285-86.

[130] *See id.* at 288 ("[T]o the extent that the SCA purports to permit the government to obtain such emails warrantlessly, [that portion of] the SCA is unconstitutional.").

[131] In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917, at *5 (D.Kan. 2012) ("The Court finds the

and the state of Washington Court of Appeals.[133] Other courts have applied *Warshak* to find a reasonable expectation of privacy in stored Facebook messages,[134] text messages,[135] faxes,[136] and password-protected websites.[137] Other courts have presumed Fourth Amendment protection in e-mails: In evaluating the lawfulness of warrants obtained to collect e-mails pursuant to Section 2703(a) of ECPA, those courts have mostly not even paused to consider whether the communications might not be unprotected.[138] In contrast, no court has reached the contrary result. *Warshak* has been adopted by every court that has squarely decided the question. The case law is not entirely settled, I concede. Only one federal court of appeals has squarely addressed the issue. But the trend in the case law is to recognize fairly broad Fourth Amendment protection, backed by a warrant requirement, for stored contents such as e-mails.

---

rationale set forth in *Warshak* persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received thorough an electronic communications service provider.")

[132] United States v. Ali, 870 F.Supp.2d 10, 39 n.39 (D.D.C. 2012).(recognizing a reasonable expectation of privacy in the content of emails).

[133] State v. Hinton, 280 P.3d 476, 483 (Wash.App. Div. 2 2012) ("While *Warshak* does not aid Hinton, its comparison of e-mails with traditional forms of communication is helpful and we adopt it to hold that text messages deserve privacy protection similar to that provided for letters.")

[134] R.S. ex rel. S.S. v. Minnewaska Area School Dist., No. 2149 --- F.Supp.2d ----, 2012 WL 3870868, at *11-12 (D.Minn. 2012) ("The Court agrees that one cannot distinguish a password-protected private Facebook message from other forms of private electronic correspondence.").

[135] State v. Hinton, 280 P.3d 476, 483 (Wash.App. Div. 2 2012) ("While Warshak does not aid Hinton, its comparison of e-mails with traditional forms of communication is helpful and we adopt it to hold that text messages deserve privacy protection similar to that provided for letters.")

[136] In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917 at *5 (D.Kan. 2012)

[137] United States v. D'Andrea, 497 F. Supp.2d 117, 121 (D. Mass. 2007).

[138] See, e.g., United States v. Cioffi, 668 F.Supp.2d 385, 396 (E.D.N.Y. 2009); United States v. Bowen, 689 F.Supp.2d 675, 682 (S.D.N.Y. 2010); United States v. McDarrah, 2006 WL 1997638, at 9-10 (S.D.N.Y. 2006), aff'd United States v. McDarrah, 351 Fed.Appx. 558 (2d Cir. 2009). *But see* In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917, at *3-5 (D. Kan. 2012) (discussing the Fourth Amendment question).

The existence of full constitutional protection for the contents of remotely stored Internet communications significantly lessens the need for statutory protections that were at the heart of the 1986 statute. In a historical sense, ECPA has served its purpose: Congress intended it as a stopgap measure designed to impose statutory protections until Fourth Amendment precedents became established. Now that the courts have stepped in and begun to regulate government access to stored contents, ECPA need no longer do so. Statutory protections are still needed to regulate nongovernmental access to contents of communications that the Fourth Amendment will not reach.[139] But recent Fourth Amendment rulings suggests that the focus of the statute can turn more to non-content information such as logs and IP addresses that remain outside the Fourth Amendment.[140]

Granted, the constitutional protections remain tentative: The Supreme Court has not yet spoken. There is significant value in statutory protections before the constitutional precedents are clearly established.[141] At the same time, another constitutional development handed down after ECPA renders its content protections a mixed bag. In *Illinois v. Krull*,[142] the Supreme Court held that the exclusionary rule does not apply when the police conduct a search in reasonable reliance on statutory authority. An Illinois state statute allowed the police to conduct warrantless inspections of automobile salvage yard records.[143] After the Illinois Supreme Court ruled the searches pursuant to the statute unconstitutional, the United States Supreme Court held that the exclusionary rule nonetheless did not apply because the officers had reasonably relied on the statute authorizing warrantless searches.[144]

---

[139] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (noting that the Fourth Amendment does not regulate private searches).

[140] *See* United States v. Forrester, 512 F.3d 500, 510-11 (9th Cir. 2008) (holding that non-content information such as IP addresses and the to/from information of e-mail addresses is not protected by the Fourth Amendment).

[141] *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805, 857-87 (2004).

[142] 480 U.S. 340 (1987).

[143] *See id.* at 343.

[144] *See id.* at 355.

Under *Krull*, statutory privacy regulations such as ECPA's protections for contents of communications cut both ways. Because ECPA's provisions do not include a statutory exclusionary rule for either access to stored communications or the interception of computer communications, criminal defendants seeking suppression of evidence must rely on the Fourth Amendment. But *Krull* complicates efforts to clarify Fourth Amendment law through suppression motions by allowing courts to deny motions to suppress under the good-faith exception of *Krull* without resolving how the Fourth Amendment applies. That largely explains why only one federal circuit court to date has directly addressed Fourth Amendment protections in e-mail. Litigation over Fourth Amendment rights in e-mail rarely reach the merits in light of *Krull*.[145] Eliminating content protections under ECPA may paradoxically speed up the process of more firmly establishing the apparent strong constitutional protections. And once those protections are established, content protections with less process with a warrant are no longer necessary because the Fourth Amendment already provides the needed protection.

(D) Particularity and Minimization of Internet Communications and Records

The fourth distinctive feature of ECPA that is outdated today is the absence of any reference to the particularity, minimization, or limits on disclosure of records obtained. Particularity is a concept from Fourth Amendment law that refers to the scope of searches.[146] The text of the Fourth Amendment states that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."[147] Particularity limits the scope of searches and therefore helps avoid fishing expeditions. In the Fourth Amendment setting, for example, it ensures that searches can be directed at a single house rather than an entire city block (or an entire city), as well as for specific evidence instead of any evidence.

---

[145] I discussed how the *Krull* good-faith exception has delayed the caselaw on the Fourth Amendment implications of government access to e-mail in Orin S. Kerr, *Fourth Amendment Remedies And Development Of The Law: A Comment On Camreta v. Greene And Davis v. United States*, 2011 Cato Sup. Ct. Rev. 237, 257.

[146] *See* Maryland v. Garrison, 480 U.S. 79, 84-85(1987).

[147] U.S. Const. Amend. IV.

Applying the particularity concept to records collected from Internet providers raises the following question: After the government satisfies the relevant threshold to obtain records, how many records does the government then collect? This question did not arise when ECPA was drafted because few records existed to be accessed. At that time, storage was expensive and detailed records were not kept. Companies generally deleted copies of e-mails read by users to save space for other messages.[148] As a result, Congress never considered the question of how particular records could be. Investigators simply could not collect enough records to make particularity an issue, so the statute contains no express limits on the particularity of orders to obtain information.

The absence of any reference to particularity of court orders creates considerable headaches today. Storage has become cheap, and providers store everything by default. As a result, the scope of records obtained has become vitally important. Recall the example of the court order to obtain the contents of a single Facebook account. When the Boston Police Department released documents investigators had collected pursuant to ECPA to solve the case of the so-called "Craigslist Killer," the 72-page report of the Killer's Facebook account revealed every single message, photo, and mouse click ever associated with the account.[149] Every visit to every page, every viewing of every picture, and every click on every link was documented with a specific entry in a log file. A single court order disclosed everything to the police as a matter of routine practice without any concern about the particularity of communications sought.

ECPA is also silent about court orders that extend beyond a single user to encompass hundreds or even thousands of users. A surveillance practice known colloquially as a "cell tower dump" illustrates the problem.[150] Cell phones must maintain contact with local cellular towers to route communications between the phones and the phone network.[151] As a result, cell phone companies generate

---

[148] *See* Part I.B, *supra*.

[149] The report is available at http://www.scribd.com/fullscreen/88465177?access_key=key-247mvzrfrh1m1azdsoai.

[150] *See, e.g.,* In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d), --- F.Supp.2d ----, 2012 WL 4717778, at *1 (S.D.Tex. 2012).

[151] *See* id.

records as to which phones are in communication with which towers at particular times. This so-called "cell-site" data provides a rough indication of the location of the phone, and thus the location of its owner. A "cell tower dump" refers to obtaining records of all customers whose phones were in contact with a cell tower over a particular window when a crime occurred.[152] For example, if a bank robbery occurred on Main Street at 3pm, a cell tower dump might allow the government to obtain records of every cell phone user whose phone was in contact with local towers near Main Street at that exact time.

In its current form, ECPA says nothing about the particularity of cell tower dumps. The statutory text merely says that, on a proper showing of cause, the government may obtain an order "requir[ing] a provider of electronic communication service . . . to disclose . . . information pertaining to a subscriber to or customer of such service."[153] If the phrase "a subscriber to or customer of" means that each order must be limited to a single customer, then ECPA does not allow cell tower dumps at all. But if tower dumps are allowed – which courts so far have assumed – then the statute is remarkably tone deaf to the scale of the privacy invasion. Imagine the police believe a house was robbed between noon and 6pm on a busy city block. Can the police obtain records for the entire six-hour window, potentially implicating thousands of users? And how many towers can the records concern? And what happens to the data that the government obtains, very little of which is likely to be relevant to the investigation?[154]

Constitutional doctrine can address the particularity problem in ECPA in the narrow context of contents already protected by Fourth Amendment. In one recent case, for example, a magistrate judge refused to issue a search warrant sought under ECPA for the contents of an e-mail account and a fax account because it was insufficiently particular.[155] The warrant applications asked for "all records and other

---

[152] *See* In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d), --- F.Supp.2d ----, 2012 WL 4717778, at *1 (S.D.Tex. 2012).

[153] 18 U.S.C. 2703(c)(1).

[154] In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d), --- F.Supp.2d ----, 2012 WL 4717778, at *4 (S.D.Tex. 2012).

[155] In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917, at *10-11 (D. Kan. 2012).

information regarding the account"[156] including "including deleted communications, as well as all records and information regarding identification of the email or fax account, and other information stored by the account user, including address books, contact lists, calendar data, pictures and files."[157]

This was "too broad and too general"[158] to satisfy the Fourth Amendment, the Magistrate Judge held. A warrant for the entire contents of the account was "best analogized to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime."[159] Because the Fourth Amendment would not permit such a warrant for the post office, it could not "permit a similarly overly broad warrant just because the information sought is electronic communications versus paper ones."[160]

But if the Fourth Amendment particularity requirement can address the scope of searches when contents are protected by the Fourth Amendment, it cannot serve that function with non-content information outside the scope of constitutional protection.[161] The existing ECPA statute simply fails to address the allowed scope of records that can be sought under the statute.

(E) The Territoriality of ECPA

The final outdated dichotomy in ECPA is its territorial scope. In 1986, communicating over computer networks occurred mostly in the United States. Commercial providers such as Compuserve provided United States users with e-mail and bulletin board services reachable by telephone and modem with United States numbers, but international calling rates made such services all but inaccessible outside the United

---

[156] *Id*. at *8.

[157] *Id*. at *9.

[158] *Id*. at *8.

[159] *Id*. at *9.

[160] *Id*. at *9.

[161] *See* United States v. Forrester, 512 F.3d 500, 510-11 (9th Cir. 2008) (holding that non-content information such as IP addresses and the to/from information of e-mail addresses is not protected by the Fourth Amendment).

States.[162] The United States government had established ARPANET, which eventually morphed in to the Internet.[163] But its use was heavily oriented towards the United States.[164] As a result, the territorial scope of the statute did not arise in the debates over ECPA. Congress was focused on the rights of United States computer users and United States services. But the possibility that individuals outside the United States might use U.S.-based services – or that individuals inside the United States might used services based abroad – never arose.

Surprisingly few court decisions have addressed the current territorial scope of ECPA. Most of the relevant precedents involve the scope of the Wiretap Act that ECPA modified. Courts have held that the telephone wiretapping provisions of the Wiretap Act only apply to interceptions inside the United States.[165] Courts have justified this territorial limit on two grounds. The first ground is "the canon of construction which teaches that, unless a contrary intent appears, federal statutes apply only within the territorial jurisdiction of the United States."[166] The second ground is that the Wiretap Act only contains provisions for United States courts issuing wiretap orders in their jurisdictions, which suggests at Congressional intent for the statute to apply only inside the United States.[167] As a result, the

---

[162] The cost of an international telephone call in the 1980s was measured in dollars per minute, making such access out of reach to most users.

[163] Reno v. American Civil Liberties Union, 521 U.S. 844, 850-51 (1997).

[164] Even by the time of the trial in *Reno v. ACLU*, 60% of Internet servers were located in the United States. *See id.* at 850.

[165] *See* United States v. Toscanino 500 F.2d 267, 279-80 (2d Cir. 1974); United States v. Peterson, 812 F.2d 486, 492 (9th Cir.1987) (holding that the Wiretap Act "has no extraterritorial effect" and does not apply to wiretapping of telephones in Thailand).

[166] *See* United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975).

[167] *See id*. As a district court explained in United States v. Angulo–Hurtado, 165 F. Supp. 2d 1363, 1369 (N.D. Ga. 2001):

> Congress intended Title III to protect the integrity of United States communications systems against unauthorized interceptions taking place in the United States. If Congress had meant to require law enforcement agencies to satisfy Title III for interceptions conducted outside the United States, it would have provided some mechanism by which agents could obtain such approval. Congress did not do so.

Wiretap Act does not regulate any interceptions occurring outside United States borders.

The sole precedent on the territorial scope of the Stored Communications Act provisions of ECPA is a single unpublished district court decision, *Zheng v. Yahoo! Inc.*[168] In that case, political activists in China claimed that the Chinese government had tortured and detained them after Yahoo's Chinese affiliate "Yahoo! China" had disclosed identifying information about them to the Chinese government. The district court rejected the plaintiff's claim that the disclosure violated ECPA on the ground that ECPA does not apply to disclosures outside the United States.[169] The court relied heavily on the reasoning of the cases interpreting the territoriality of the Wiretap Act.[170] It also noted that the enactment of ECPA did not contain any provisions rejecting that traditional territorial scope: "The ECPA did not amend the portion of the Wiretap Act that made no provision for obtaining authorization for wiretaps in a foreign country, nor did the ECPA, in amending the Wiretap Act and creating the SCA, reference in any manner activities occurring outside the United States."[171]

Although the territorial scope of ECPA was not the focus of attention when the statute was passed, it has since become tremendously important. Today's Internet is truly global. A computer user can as easily access a website across the world as one across the street. Servers can be located anywhere, even thousands of miles away from company headquarters. For example, the servers hosting the most popular Internet poker sites serving players all around the world are located in a nondescript building on an Indian reservation not far from Montreal, Canada.[172] Or at least that is the case today: The location could change at any time.

The reality of global access means that U.S.-based Internet services often have a heavily foreign customer base. Consider Gmail,

---

[168] 2009 WL 4430297, No. C–08–1068 MMC (Dec. 2, 2009).

[169] *See id.* at *4.

[170] *See id.* at 2 (citing United States v. Peterson, 812 F.2d 486, 492 (9th Cir.1987); United States v. Toscanino, 500 F.2d 267, 279 (2nd Cir.1974); Stowe v. Devoy, 588 F.2d 336, 341 (2nd Cir.1978)).

[171] *Id*. at *3.

[172] http://news.cnet.com/60-minutes-report-how-online-gamblers-unmasked-cheaters/

the popular e-mail service provided by Google. Google is headquartered in California. But Gmail's business is truly international, and slightly less than 30% of Gmail's users reside in the United States.[173] This chart shows the percentage of Gmail's users that are in a handful of different countries as of 2012:[174]

Country	% of Gmail Users
United States	29.7%
India	8.9%
Japan	3.4%
Russia	3.3%
Brazil	3.2%
United Kingdom	2.9%
China	2.7%
Iran	2.6%

Facebook's user base is even more heavily foreign than is Gmail's user base. To be sure, using Facebook has become as American as apple pie: About 54% of Americans presently have a Facebook account.[175] At the same time, only about 16% of Facebook's users are located in the United States.[176] The rest, about 84%, access Facebook from abroad. For United States-based services like Gmail and Facebook, United States users form a small subset of its global customer base.

The friction between the territorial ECPA and the global Internet creates two major puzzles that ECPA's drafters could not have foreseen. First, what does it mean for ECPA to apply only inside the territory of the United States? In today's networked environment, company headquarters can be located in one country; employees with access to the data can be located in a second country; the data can reside in a

---

[173] *See Gmail Usage Per Country*, available at http://www.appappeal.com/maps/gmail.

[174] *See id.*

[175] See Quentin Fottrell, *Facebook Loses 1.4 Million Active Users in U.S.*, Marketwatch, January 15, 2013, available at http://articles.marketwatch.com/2013-01- 15/finance/36346107_1_active-users-facebook-social-media (last visited March 5, 2013).

[176] *See id.* (reporting that, as of January 2013, about 167 million of Facebook's 1 billion users are located in the United States).

third country; and the party seeking access to the data could be located in a fourth country. All of the data could of course be easily sent electronically from any place in the world to any other place. What determines territoriality? The location of the data? The company? The employee? Or the requesting party?[177] Imagine a person in Mexico who seeks the e-mails of another person in Mexico, and he does so by contacting employees in France who work for an Internet company headquartered in Belgium that hosts its servers in the United States. If the company discloses the records, is that disclosure inside the United States for purposes of the territoriality of ECPA? Does it matter if the French employees first have the data e-mailed to them and then disclose the communications from France to Mexico? ECPA offers no answers to such questions.

Indeed, the very idea of online data being located in a particular physical "place" is becoming rapidly outdated. From the standpoint of network design, a person's e-mail files could be fragmented and the underlying data located in many places around the world.[178] The e-mails could only exist in recognizable form when they are assembled remotely. That assembly could occur anywhere at the direction of someone who could be located anywhere else. If the location of the stored data governs under ECPA, what is the location of e-mails that were stored in fragments all around the world?

A second puzzle created by the mismatch of the territorial statute and the global Internet is how the statute deals with foreign government access. The frequency by which services like Gmail are used by individuals outside the United States explains why foreign governments often seek access to records or contents held by U.S.-based service providers concerning individuals abroad. Under the Ninth Circuit's decision in *Suzlon Energy Ltd. v. Microsoft Corp.*,[179] the location of the customer or subscriber has no bearing on that

[177] Courts have encountered similar questions in the course of identifying the location of an intercept under the Wiretap Act for purposes of obtaining a wiretap order in a particular district. *See* United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997) (Posner, J.)

[178] John Villasenor & Vivek Mohan, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. Pa. J. Con. L., 11, 20-22 (2012).

[179] 671 F.3d 726 (9th Cir. 2011).

individual's ECPA rights.[180] Individuals outside the United States who use Gmail from abroad have the same statutory rights as United States citizens using the service from inside the United States.

At the same time, foreign governments often believe that their local priorities and local laws should control. For example, in 2007, prosecutors in Belgium brought criminal charges against the United States-based provider Yahoo for its failure to comply with records sought about customers in the Netherlands that Belgian prosecutors suspected of criminal activity.[181] Yahoo's defense was based in part on ECPA: According to Yahoo!, it was a United States provider governed by United States law. The criminal case against Yahoo is still pending in the Belgian courts.[182] But the lesson is clear: The global Internet requires privacy laws that account for the demands of governments around the world rather than just the United States.

What rules currently apply when a foreign government approaches a United States-based provider and demands information for a foreign investigation about a foreign user? In its current form, ECPA does not recognize foreign governments as governments at all. Government entities are defined as "department[s] or agenc[ies] of the United States or any State or political subdivision thereof,"[183] thus excluding governments abroad. This means that foreign governments cannot obtain mandatory process using foreign court orders.[184] Further, the presumptive ban on the disclosure of contents of communications will apply to disclosure sought by foreign governments just as it does to disclosure sought by private entities.[185] At the same time, because ECPA permits providers to disclose non-content

---

[180] *See id*. at 729-30.

[181] *See* Tanguy Van Overstraeten & Ronan Tigner, *Belgium - Yahoo! Saga Continues: Yahoo! Must Not Hand Over Personal Data to the Public Prosecutor*, Linklaters Technology, Media & Telecommunication News, January 30, 2012, available at http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-Newsletter-January-2012/Pages/9_Belgium-Yahoo!-saga-continues-Yahoo-personal-data-public-prosecutor.aspx (last visited March 5, 2013).

[182] *See id.*

[183] 18 U.S.C. § 2711(4)

[184] 18 U.S.C. § 2703 (providing for means of compelling information for government entities).

[185] *See* 18 U.S.C. § 2702(a),(b).

information to non-government entities,[186] providers can disclose non-content information to foreign governments at their discretion. As a practical matter, then, foreign governments can often obtain non-content information using foreign court orders: The providers have a choice to disclose the information or not, and they may do so in response to a legitimate court order even thought the order is not binding in the United States.

The picture is more complicated when foreign governments seek content information. Three basic options exist. The first two paths work with the statute and are clearly legal; the third path tries to work around the statute and is probably unlawful. The first option is for foreign governments to work with the United States government and to use Mutual Legal Assistance Treaties or letters rogatory to seek information from providers using official diplomatic channels.[187] This process generally remains slow and laborious, as it requires the cooperation of two governments when a case may not be the priority of the second.[188]

A second option is for foreign governments to persuade United States officials to open a domestic investigation and obtain United States court orders binding in the United States. Domestic officials can then turn over the fruits of the court orders to the foreign authorities. The procedure can be very quick, but it requires the foreign crime to also be a United States offense.[189] Further, it requires United States

---

[186] *See* 18 U.S.C. § 2702(c)(6) (permitting disclosure of non-content information "to any person other than a governmental entity").

[187] *See generally* Orin S. Kerr, Computer Crime Law 752-59 (3d ed. 2013) (discussing the legal regime for letters rogatory and mutual legal assistance in computer crime cases).

[188] *See id.*

[189] Notably, United States criminal laws have been expanded extraterritorially to enable United States assistance to foreign governments. By making the crime outside the United States a crime inside the United States, investigators in the United States can open a domestic investigation and assist foreign governments when evidence happens to be located inside the United States. *See* Computer Crime and Intellectual Property Section (CCIPS), Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001 (2001), quoted in Kerr, *supra* note 187, at 732 (discussing the extraterritorial expansion of the Computer Fraud and Abuse Act as a way to assist foreign computer crime investigations).

investigative authorities to approve of the investigation and consider it a sufficient priority (either to further its own interests or to advance comity interests in cooperation) to merit the resources.

The third option is legally dubious but nonetheless deserves discussion: A provider may try to export the data to a representative or an affiliate outside the United States. As soon as the data is outside the United States, the representative or affiliate can disclose the data under the rationale that the disclosure is no longer inside the United States and therefore no longer regulated by ECPA. This option is likely unlawful because it merely breaks the unlawful disclosure into two steps. It would be surprising if providers could circumvent ECPA's territorial limits on disclosing contents without a court order by first e-mailing it to a corporate representative abroad. At the same time, the question becomes harder if companies design their networks to achieve the same result. For example, imagine foreign governments pressure United States companies to design their networks to store a second copy of data outside the United States. Does ECPA apply to disclosures from the second copy abroad? There are no decisions on the issue and no statutory text that clearly governs it.[190] ECPA simply was not written with the possibility of such technology in mind.

III. Crafting A Next Generation Privacy Act

If Congress could start from scratch and enact a new privacy statute, what would that statute look like? This section offers a set of principles that such a new privacy statute should adopt. It argues that a new privacy statute should be based on four principles. *First*, Congress should create a new statute to govern Internet privacy that imposes a uniform requirement for compelled access to remotely-stored contents held for a customer or subscriber. *Second*, Congress should create a particularity requirement for compelled access to non-content. *Third*, Congress should impose minimization rules on all contents of communications obtained by investigators. And *fourth*, Congress should

[190] For example, imagine a network provider is pressured by the foreign government to design its network such that it keeps a copy of its messages in the home country to be regulated by its laws instead of ECPA? Does the network design govern?

impose a territoriality regime based on the location of the user, such as one that provides full protections for users based on the United States and a permissive regime of disclosure to foreign legal process for users based abroad.

(A) Congress Should Enact a Uniform Requirement for Access to Any Remotely-Stored Contents Held by or For a Customer or Subscriber

The first principle of the new statute should be the imposition of a uniform set of rules to govern access to contents held by or for a customer or subscriber. The core theme animating electronic privacy statute is the problem of third party control. Users of computer networks necessarily place information in the control of others. The new statute should confer one standard for access to the contents of data held by or for a customer or subscriber. Whenever access is sought to such data, the law should impose a single legal standard for access.

This approach would abolish the existing distinctions between protections against "real time" access currently covered by the Wiretap Act and the regulation of stored access presently covered by the Stored Communications Act. As explained in Part II, the low storage costs of electronic information has led to a convergence between the privacy implications of real-time and stored access. The new statute should treat them in the same way and impose the same standard for access. Eliminating the distinction between real-time and stored access has the added benefit that the distinction is famously difficult to apply for computer and Internet communications. Courts have struggled to articulate just how quickly and how often access needs to occur for it to treat as "contemporaneous" and therefore fit under the Wiretap Act.[191] Under my proposed approach, this metaphysical line would be eliminated.

My approach also eliminates the existing ECS/RCS distinction and imposes a uniform standard for all providers. All third-party storage of communications should lead to the same protection, regardless of whether the provider acts as an e-mail host, a cloud provider, or a search engine. The problem of third-party storage is a general one. In all of these cases, a user shares the contents of their

[191] *See* LaFave, *supra* note 2, at § 4.6(b).

private communications with a third-party service that is not the intended human recipient of the message. In all of these settings, users should receive the same privacy protections against disclosure by the third-party services about their communications. All providers should be covered, and all should be covered by the same rule. At the very least, the presumption should be that the same level of privacy protection applies regardless of the means of access: Deviations from that norm should require significant justification.

Of course, harmonization requires identifying the uniform standard by which contents would be obtained. Standards might be harmonized up, harmonized down, or a harmonized somewhere in the middle. I have argued elsewhere that Fourth Amendment ordinarily requires a probable cause warrant for government compelled access to contents,[192] and that traditional Fourth Amendment standard provides one natural starting point. The "super warrant" standard imposed for real-time wiretapping confers the highest statutory protection under criminal surveillance laws and provides a second possible point of reference.[193] Because this paper is a thought experiment, I will not attempt to answer where the ideal line should be drawn. But wherever it is drawn, existing technology counsels in favor of a uniform standard for compelled access to contents.

(B) Particularity Requirements for Non-Content Data Could Be Imposed Based on a Concept of Customer-Hours

The second principle of the new statute should be the adoption of particularly requirements. The ECPA statute pays no attention to particularity because few records existed that could be collected when the statute was enacted. The scale of data available was sufficiently limited that scale played little role. That is no longer true. Today the default has become that all data is stored. As a result, the threshold of cause that the government must satisfy to obtain information has to be

---

[192] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005 (2010).

[193] *Cf.* Susan Freiwald, *Online Surveillance: Remembering The Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9 (2004) (arguing that Internet surveillance should probably adopt the highly protective standards of the Wiretap Act).

matched with a second question of how much information can be obtained when that cause has been established.

It helps to divide the proper approach to particularity into two parts: Contents and non-content information. In the case of contents, the Fourth Amendment applies and the constitutional particularity requirement already requires the government to satisfy traditional Fourth Amendment particularity concerns.[194] Although statutory particularity could be imposed, the Fourth Amendment protections already exist and should serve that function. The harder question, and the one that is more important for purposes of a new statute, is what kind of particularity requirement the law should impose for non-content information not protected by the Fourth Amendment.

Identifying the proper particularity standard for non-content information is difficult because such records exist in many different forms. Some non-content records are more sensitive than others. A list of every e-mail address that a person e-mailed together with the time each e-mail was is more sensitive than merely the name on the account. Further, as the example of cell tower dumps reveals, investigators often want records from many different users at once. As a result, particularity might impose limits on the number of type of records from a particular user or from a range of users. The question is, what principle should Congress use to limit the scope of non-content records access? Should it be the overall number of records collected, perhaps with limitations on a particular number of records obtained per order? Or perhaps limitations should be imposed based on the number of accounts obtained?

There is no perfect answer to this question. However, one approach to particularity worth considering for non-content information is the concept of *customer-hours*. In an environment of widespread and detailed record keeping, the best way to measure the scope of access to metadata is by identifying the time a customer used the service. If providers collect everything, the time over which the collection occurs most effectively identifies the scope of the metadata

---

[194] *See, e.g.,* In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917, at *4-5 (D. Kan. 2012). Of course, Congress could enforce a particularity limit that is more restrictive than a constitutional limit.

collected. Further, because the government often seeks the records of multiple users, the records from a time period for one user are in effect a substitute for the records from a period for a different user. As a result, imposing a particularity requirement based on a defined maximum number of customer-hours may provide the best way to limit the scope of non-content records accessed.

An illustration might help explain how this would work. Imagine that Congress sets the threshold for access to non-content records using a standard akin to the existing 2703(d) standard of specific and articulable facts that the records obtained would be relevant and material to an ongoing investigation.[195] Congress could then impose a particularity limit of a specific number of customer-hours for each court order. To pick a number, imagine that a single order is capped at 500 customer-hours. If the government satisfies the threshold showing of cause, it can obtain all the non-content records for a single user for 500 hours, the equivalent of about 21 days. Alternatively, the government could ask for the records of two customers for 250 hours each, or five users for 100 hours each. We can also apply this approach in the context of a cell tower dump. A cell tower dump might reveal records from 1,000 customers. In that case, the particularity limitation of 500 customer-hours would limit the government's access to 30 minutes of time. If the government sought information from more towers, or chose towers with particularly high usage, the government could still obtain the order but only for an even shorter time window.[196]

(C) Minimization Rules Should Apply to All Obtained Contents of Communications

The next principle of the new statute is that minimization principles from the Wiretap Act should apply to access to all contents. Existing law adopts a bifurcated privacy regime. Under the Wiretap Act, lawful access to communications comes with strings attached.[197] Even after obtaining a lawful wiretap order, agents are required to screen

[195] *See* 18 U.S.C § 2703(d).

[196] Granted, there could be implementation issues with this standard if the number of individuals involved were unknown or varied considerably over time.

[197] *See* Part IB, *supra*.

communications ex ante and then carefully limit disclosure ex post.[198] Under the SCA, a court order requires the provider to provide the government with the entire contents of the account. The government is then free to look through all of it.

This was understandable back when few Internet communications were stored. But in a world of total storage, the present absence of legal rules on minimization has become an anomaly. Every collection of contents of communications should impose the same requirements of minimization regardless of whether they involve access to real-time or stored communications. Importantly, the concept of minimization need not mirror its application in the telephone setting. Here the Senate Report accompanying ECPA was remarkably prescient. In the course of explaining how the minimization requirement might apply to wiretaps of computer communications, the report writes:

> It is impossible to "listen" to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation. For instance, a page displayed on a screen during a computer transmission might have five paragraphs of which the second and third are relevant to the investigation and the others are not. The printing technology is such that the whole page including the irrelevant paragraphs, would have to be printed and read, before anything can be done about minimization.
>
> Thus, minimization for computer transmissions would require a somewhat different procedure than that used to minimize a telephone call. Common sense would dictate, and it is the Committee's intention, that the minimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete all nonrelevant materials and disseminate to other officials only that information which is relevant to the investigation.[199]

As the Ninth Circuit has recognized, minimization for electronic communications requires filtering:[200] Someone must go through the

---

[198] *See id.*

[199] S.Rep. No. 99-541, at 30-31 (1986).

[200] *See* United States v. McGuire, 307 F.3d 1192, 1202 (9th Cir. 2002) ("We interpret Congress's "common sense" idea of electronic minimization to mean that law

records and find the pertinent communications. The details of how minimization should be performed are not my focus here, but some kind of minimization standard should apply to the review of protected contents.[201]

(D) Congress Could Establish a Two Part User-Based Regime for Territoriality

The fourth and final principle of a next generation privacy act would be the establishment of an explicit regime for the territoriality of the statute and the mechanisms for foreign government access. Congress could do that in several ways. The many options reflect the several major variables that govern territoriality, including the location of the information, the location of the user, and the location of the company that hosts the information. Further, Congress must decide how to treat foreign government access. Congress could allow United States-based companies to disclose communications or records pursuant to foreign government orders, or it could require governments to comply with Mutual Legal Assistance Treaties instead. Alternatively, Congress could regulate territoriality by adopting express rules as to when providers can or must design their networks in ways that go outside U.S. territory to subject communications to foreign government access.

Based on existing technology, the best of the available options is to focus privacy protections on the perceived location of the user. Providers usually have rough sense of the location of their customers.[202] Users often can select a language, and they also reveal IP addresses every time they access a provider's services. IP addresses can be manipulated, of course, but it is often possible to gauge the rough

---

enforcement in some circumstances may look at every communication. Congress intended that the pool of investigative material be filtered.").

[201] I have argued elsewhere that the plain view exception should not apply to digital evidence searches, including searches through contents of communications obtained form third-party providers. *See* Kerr, *supra* note 124, at []. I continue to adhere to that view, although I will not repeat the argument here.

[202] *See, e.g.,* Marketa Trimble, *The Future Of Cybertravel: Legal Implications Of The Evasion Of Geolocation* 22 Fordham Intell. Prop. Media & Ent. L.J. 567, 586-99 (2012).

location of a user from the IP address used to access the network.[203] The combination of language and IP address gives providers a general sense of the country used to access their network by each customer.

A rule based on the location of the user is far from ideal, to be sure. Some customers access services from multiple countries.[204] Others access services using anonymized IP addresses, making their location difficult to identity. Nonetheless, providers generally can separate out at least most of their U.S. based customers from customers in other countries. And if user location can be difficult to identify, the remaining options seem worse. In a global network, the location of the data is arbitrary and increasingly unknowable. The location of the company holding the data is equally arbitrary and difficult to apply given that multi-national companies can have affiliates and branches anywhere. A standard based on perceived user location is problematic, but it seems less problematic than the alternatives.

Further, difficulties in identifying location can be addressed through presumptions and standards of proof. For example, the rule might be that a person is presumed to be inside the United States unless there is clear and convincing evidence that the user is outside the United States. The standard could also incorporate a time element, looking to the person's location over the previous month or year to determine where the person is located. None of these standards will be perfect, but they may provide a way to implement a location-based standard in a way that makes such an approach better than the alternatives.

Focusing on user location could enable a two-part solution to the territoriality problem along the following lines. First, Internet providers either based in the United States or that do business in the United States must follow United States privacy law with respect to their United States-based users. That requirement would apply regardless of where information is technically stored. Under my

---

[203] *See id*.

[204] For example, a user might travel around the world, accessing the network from various places. In that case, it may be difficult or impossible to definitively associate the person with a particular home country. At the same time, the use of defaults may solve this problem. For example, the law could presume that a user of a United States service is located in the United States unless the evidence indicates otherwise with some clarity.

proposal, privacy protections should follow the user instead of the data: All state or federal government access to information about United States users should comply with United States law. So long as a company with a presence in the United States has communications belonging to United States-based customers, that company should have to follow United States law imposing a warrant requirement on access. Internet providers in the United States would therefore be free to design their network to optimize the engineering problem of storage and service without worrying about the implications for the privacy of their United States-based users. And users in the United States would know that all of their use of United States services would receive the full protection of United States law.

The second part of the solution would focus on the rights of users based outside the United States. For users outside the United States, the law should allow but not require Internet providers to disclose contents and non-content information pursuant to foreign legal process in the country associated with the account holder. If French authorities in France produce a valid court order pertaining to a French user, United States providers should be permitted to comply with the order. This approach places some burden on providers that service foreign customers to learn enough about foreign legal process to understand foreign court orders. But importantly, the disclosure would be permissive rather than mandatory. Providers that chose not to comply with foreign court orders would not be required to do so, allowing providers to opt out of foreign disclosure if they wished.

Enacting a regime of permissive but not mandatory disclosure for foreign legal process pertaining to foreign users provides important flexibility given the wide range of different legal standards and foreign governments. If disclosure were made mandatory, a totalitarian government with no privacy laws could force United States providers to disclose contents pertaining to democratic activists and critics of the regime. On the other hand, if disclosure were forbidden, even democratic governments with highly protective privacy laws would be forced to always go through cumbersome legal processes such as letters rogatory and MLATs to obtain records in routine cases. A permissive regime allows United States-based providers to choose which countries should be deemed sufficiently protective and democratic to have their legal process honored. And because that legal process would only apply

to users located in the country where the user is located, the law would both protect United States users and permit providers to be confident that they were disclosing foreign records appropriately in each case.

More, broadly, a user-focused solution to territoriality recognizes the inherently global nature of today's Internet. It no longer makes sense to think of data as being in a particular "place" given that data can be sent anywhere or stored in pieces around the world. In contrast, users remain rooted in the physical world and are governed by the sovereign interests of that place. Hinging privacy protections on the location of the user ensures that users receive the same localized protections in the cloud that they do in their homes.

Conclusion

Congress rarely enacts sweeping reforms. Slow evolutionary change ruffles fewer feathers than does wholesale revision. If Congress could enact a new privacy law today, however, the rapid pace of technological change since 1986 would lead to a rather different set of statutory privacy laws than exist today. The law would adopt a single uniform standard for access to contents; focus much more on particularity and minimization; and deal explicitly with the problem of extraterritoriality.

Whether or not Congress is able to enact a wholesale revision of the privacy laws, it should realize that substantial reform is likely to be needed in our lifetimes. The first federal surveillance law was the Communications Act of 1934; It was replaced by the Wiretap Act 1968, which was supplemented considerably by ECPA in 1986. Since that time, communications networks have become only more important to American life. The incredible growth of the Internet and is rapid transformation from a toy to an essential part of daily life has made the accuracy and timeliness of the electronic privacy laws more important than ever before.

The vital importance of computers and the Internet tasks Congress with keeping the privacy laws up to date. The Internet of today has diverged in profound ways from the Internet that existed when Congress last enacted major reform. Whether Congress acts in

piecemeal fashion or starts from scratch, the statutory privacy laws should reflect the privacy threats and government practices of the present rather than the threats and practices of an earlier generation.