ARTICLE

THE NEXT GENERATION COMMUNICATIONS PRIVACY ACT

ORIN S. KERR†

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to regulate government access to Internet communications and records. ECPA is widely regarded as outdated, and ECPA reform is now on the Congressional agenda.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 were to repeal ECPA and enact 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 noncontent 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 U.S.-based services now serve a predominantly

† 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 presently serves 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, Ramesh Ponnuru, and Gail Kent for their helpful comments, as well as Cynthia Jordan, Robert Newlen, and David Mao at the Law Library of Congress for their support. This Article was presented as the 2013 John L. Gedid Lecture at the Widener University School of Law.

foreign customer base. A new statute would need to account for these changes.

This 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 U.S.-based users and a permissive regime for users located abroad.

INTRODUCTION

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

In recent years, ECPA has become widely perceived as outdated.[4] Senator Patrick Leahy, the Chairman of the Senate Judiciary Committee, recently announced that ECPA reform is now a "top priority."[5] His counterpart on the House side, Representative Robert Goodlatte, chairman of the House Judiciary Committee, has also endorsed the need to reform ECPA and recently held hearings on ECPA reform.[6]

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 Act's 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?

---

1 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

2 *See generally* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE §§ 4.5–4.8(e) (3d ed. 2007).

3 The major changes to ECPA following 1986 are discussed *infra* Section I.C.

4 *See* Charlie Savage, *Panel Approves a Bill to Safeguard Email*, N.Y. TIMES, Nov. 30, 2012, at B7 (noting that ECPA "is widely seen as outdated"); *see also* Brendan Sasso, *Consensus Builds for Requiring Warrant for Email Searches*, HILL'S HILLICON VALLEY (Mar. 19, 2013), http://thehill.com/blogs/hillicon-valley/technology/289035-consensus-builds-for-requiring-warrant-for-email-searches (quoting Representative Jim Sensenbrenner as saying that ECPA's requirement of only a subpoena for access to email records is "outdated and probably unconstitutional").

5 Brendan Sasso & Jennifer Martinez, *OVERNIGHT TECH: House to Consider Email Privacy Bill*, THE HILL'S HILLICON VALLEY (Feb. 27, 2013), http://thehill.com/blogs/hillicon-valley/technology/285397-overnight-tech-house-to-consider-email-privacy-bill; *see also* Sen. Patrick Leahy, Chairman, S. Judiciary Comm., The Agenda of the Senate Judiciary Committee for the 113th Congress (Jan. 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 and cybersecurity laws.").

6 *See* Sasso & Martinez, *supra* note 5 (reporting House Judiciary Committee Chairman Robert Goodlatte's commitment to "look at modernizing the decades-old Electronic Communications Privacy Act (ECPA) to reflect our current digital economy").

7 *See infra* Section I.D.

The Article contends that such a new privacy act would look quite different from the current ECPA. Network technologies have dramatically transformed 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, today's Internet is quite different from the Internet of a decade ago, often in ways that are imperceptible to the user but that 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 ECPA statute on the books today.

Two technological changes are particularly important. First, the plummeting costs of storage have changed how surveillance threatens privacy.[8] ECPA was drafted at a time when electronic storage was expensive and therefore relatively rare. Accordingly, ECPA treated real-time wiretapping as the chief privacy threat. Access to stored communications was 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 this technological change, access to stored records has become the greater privacy threat. The incredible growth of stored records renders ECPA's structure exactly backwards for the operation of modern computer networks.

Second, the Internet has become truly global.[9] ECPA was drafted when computer network usage was very heavily U.S.-based. The Act created statutory protections for U.S. users of U.S. services. Today's network usage looks dramatically different: only about ten percent of the today's global Internet usage involves U.S.-based individuals. [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 than just technology has changed: 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

---

8 *See infra* Section II.A.
9 *See infra* Section II.E.
10 *See infra* Section II.E.
11 *See infra* Section II.E.
12 *See infra* Section II.C.

statutory stand-in for uncertain Fourth Amendment protection. As the scope of Fourth Amendment protection becomes more certain, however, the statute's coverage may change with it.

As a practical matter, lawmakers rarely start from scratch when passing legislation. Amending prior laws is the norm for a variety of reasons. But if Congress were forced to enact a new privacy act, that new law ideally would be based on four principles. *First*, the new statute would impose a uniform warrant requirement for compelled access to contents held for a customer or subscriber.[13] The new statute would abolish ECPA's antiquated distinctions, 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 would treat all access to contents under the same warrant standard.

Second, the law would enact a particularity requirement for compelled access to noncontent information.[14] One approach might rely on the concept of customer-hours. When the government obtains a court order to compel records, it should not be entitled to all of a user's records—or even worse, all records of hundreds of users. Instead, each court order could be limited based on both the time coverage of the order and the number of users implicated. If the government seeks records associated with many users, it must accept the tradeoff that those records will span a shorter window of time.

Third, the new law would impose minimization limitations for contents of communications obtained by government investigators.[15] When the government collects the contents of communications pursuant to a court order, investigators should be limited in what they can access. ECPA only imposes such limits for contents obtained by real-time wiretapping, reflecting the traditional sense that real-time access poses the greatest privacy threat. 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.[16] One solution would be to focus on the location of the user, with full warrant protections for users based in the United States and a permissive disclosure regime to foreign legal process for users based abroad. A global network demands different protections for local and foreign users. Under my proposal, U.S. users would receive full warrant protection regardless of the

---

13 *See infra* Section III.A.

14 *See infra* Section III.B.

15 *See infra* Section III.C.

16 *See infra* Section III.D.

location of servers or corporate headquarters. By contrast, U.S. providers should be permitted, but not required, to disclose records pursuant to foreign legal processes for users based in the country seeking those records.

The argument will proceed in three parts. Part I introduces the history and structure of ECPA. This Part 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 based. 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. This Part begins by explaining surveillance law before ECPA. It then turns to the new technological problems that ECPA was designed to address at the time of its enactment, and it explains the basic structure of ECPA to see how it responded to these problems. This Part concludes by highlighting the limited nature of existing ECPA reform proposals and 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,[17] and it proved to be a dramatic advance over communication by telegraph. But the telephone had a serious privacy flaw. Any person with 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.[18] Some state laws prohibiting

---

17 *See* Christopher Beauchamp, *Who Invented the Telephone? Lawyers, Patents, and the Judgments of History*, 51 TECH. & CULTURE 854, 855-67 (2010) (noting that patent litigation surrounding the telephone's origins clouds the question of who invented the telephone).

18 *See* SAMUEL DASH ET AL., THE EAVESDROPPERS 25-34 (1959) (tracing phone wiretapping back to the 1890s and highlighting its growth as a practice into the 1950s); *see also* Heutsche v. United States, 414 U.S. 898, 899 (1973) (Douglas, J., dissenting) ("[W]e live in a regime where the 'dirty business' of wiretapping runs rampant.").

wiretapping emerged by 1895,[19] although the first federal statute did not arrive until the Communications Act of 1934.[20] Telephone privacy laws naturally focused on the act of "intercepting" the call—that is, breaking in on the private call by installing a listening device to monitor the communication over the wires as the call was transmitted.[21]

Congress maintained the focus on interception when it enacted the Wiretap Act in 1968.[22] The Wiretap Act replaced the Communications Act of 1934 as the federal statute governing privacy in telephone communications. Like the Communications Act, the Wiretap Act prohibits "intercepting" telephone calls between parties to a communication.[23] Unlike the Communications Act, however, the Wiretap Act includes a carefully crafted privacy regime regulating lawful interceptions.[24] That privacy regime was inspired in part by the Supreme Court's decision in *Berger v. New York*, which required any wiretapping statute to include special privacy protections against government monitoring.[25] Wiretapping raised special Fourth Amendment concerns, *Berger* had indicated, because it involved "a series of intrusions, searches, and seizures pursuant to a single showing of probable cause,"[26] rather than the "one limited intrusion" of a traditional search into physical property.[27] 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 a stringent warrant requirement for intercepting telephone calls over the wires. Interception orders can

---

19 *See* Berger v. New York, 388 U.S. 41, 46 (1967) (highlighting an 1895 Illinois law outlawing wiretapping and similar legislation enacted ten years later in California).

20 Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended at 47 U.S.C. §§ 151–609 (1934)).

21 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 communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person." Pub. L. No. 73-416, § 605, 48 Stat. 1064, 1104 (codified at 47 U.S.C. § 605 (1934)).

22 The Wiretap Act is sometimes referred to as "Title III" because it was passed as the third title of the Omnibus Crime Control and Safe Streets Act of 1968. Pub. L. No. 90-351, 82 Stat. 197 (1968). The Wiretap Act is codified as amended at 18 U.S.C. §§ 2510–22 (2006 & Supp. V 2012).

23 *See* 18 U.S.C. § 2511(1)(a) (2006) (stating that anyone who "[i]ntentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" commits a crime).

24 *See id.* § 2511(2) (2006 & Supp. V 2012) (identifying exceptions when wiretapping is lawful without a court order); *id.* § 2518 (identifying procedures for lawful interception pursuant to a court order).

25 388 U.S. 41, 57-60 (1967).

26 *Id.* at 59.

27 *Id.* at 57.

be obtained to conduct government monitoring, but they require a showing of special need, a predicate felony offense, and high-level Justice Department or state approval.[28] The Wiretap Act also includes two special rules for how the government must execute a wiretap. First, the government must engage in minimization.[29] Minimization refers to the process of trying to limit ex ante which of a suspect's communications the government will intercept.[30] 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.[31]

The second requirement is a general ban on disclosure of communications intercepted or information learned from those communications unless appropriate to the investigation.[32] Agents are not permitted to disclose information obtained from intercepted communications—even to other agents—unless it "is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure."[33] 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.[34]

B. *The Office of Technology Assessment Report and the Need for ECPA*

By the mid-1980s, Congress grew concerned about new computer telecommunications methods that fell outside the scope of existing privacy laws. In 1985, the now-defunct Office of Technology Assessment (OTA) published an influential report entitled *Federal Government Information*

---

28 18 U.S.C. § 2518(7) (2006).

29 *See id.* § 2518(5) (stating that a wiretapping order "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception"); *see also* LAFAVE ET. AL., *supra* note 2, § 4.6(h), at 496-97 (requiring the minimization of nonrelevant communications under the Wiretap Act).

30 *See* LAFAVE ET AL., *supra* note 2, § 4.6(h), at 497 (discussing how the minimization requirement "does not forbid [the] interception" of "nonpertinent communications," but requires the government to take measures to lessen their interception).

31 *See* Scott v. United States, 436 U.S. 128, 142-43 (1978) (concluding that conversations between the defendant and her mother were reasonably intercepted by government agents); *see also* United States v. Glover, 681 F.3d 411, 420 (D.C. Cir. 2012) (noting that "determining the reasonableness of minimization efforts is a fact-specific inquiry").

32 *See* 18 U.S.C. § 2517 (2006).

33 *Id.* § 2517(1).

34 *See* SEC v. Rajaratnam, 622 F.3d 159, 175 (2d Cir. 2010) (stating that, with respect to material gathered from wiretapped investigations, "the USAO [United States Attorney's Office] may not be authorized to provide these materials to [another] civil enforcement agency").

Technology: Electronic Surveillance and Civil Liberties.[35] The report noted the growth of communications sent over computers—specifically the advent of "electronic mail."[36] 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.[37] Second, users could send computer-to-computer messages over the telephone lines.[38] This generally required use of a modem to access mainframe computers, which would allow users to send a message over telephone lines to a "central computer" where the message would wait for the recipient to access and download it.[39]

Computer data transmissions and electronic mail raised several new problems not addressed by the Wiretap Act. First, the Act was largely telephone-specific.[40] The interception of computer data transmissions was not prohibited by the Wiretap Act because it only protected data transmissions that contained the sound of a human voice.[41] Data communications were not protected. This issue arose in the very first federal computer crime case when a hacker objected to being monitored using the network he had successfully invaded.[42] The Fourth Circuit held that such monitoring could not violate the Wiretap Act for several reasons, one of which was that

---

35 OFFICE OF TECH. ASSESSMENT, U.S. CONG., FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985), *available at* http://www.fas.org/ota/reports/8509.pdf [hereinafter "OTA REPORT"].

36 Notably, the issue of email privacy dominated the OTA 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 email:

> 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.

Id. at 48.

37 *Id.* at 47-48.

38 *Id.*

39 *Id.* at 48.

40 The Wiretap Act also prohibits the interception of "oral communications," which effectively prohibits the use of secret audio recording devices to record the human voice. 18 U.S.C § 2511(1)(a) (2006); *see also id.* § 2510(2) (2006) (defining "oral communication"). The oral communication aspects of the Wiretap Act, however, are not implicated by the issues raised in this Article.

41 *See* OTA REPORT, *supra* note 35, at 36 (noting that while courts had yet to rule on the matter, Title III applied to all phone conversations, regardless of whether they were in digital or analog form).

42 United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978).

computer transmissions did not contain sounds and therefore were not protected by statutory law.[43]

Second, the Wiretap Act only applied to real-time interception instead of access to stored communications.[44] This made sense with ephemeral telephone calls because the only way to access a phone call was to listen in real-time as the call occurred. However, 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 the communication's transmission.[45] As a result, the Wiretap Act did not offer any protection against government access to stored email.[46] Although the OTA Report noted that the Fourth Amendment might protect individuals against government access to their stored emails,[47] the possible scope of Fourth Amendment protection was uncertain. Any protection might not apply to backup copies held by "electronic mail companies,"[48] which the government could access.

C. *The Enactment of ECPA and Its Major Amendments*

In 1986, just one year after the OTA Report, Congress enacted ECPA to provide privacy protections for new uses of computer technologies.[49] ECPA contains three parts. The first part expands the Wiretap Act so that its prohibition on interception extends to computer data transmissions in addition to telephone calls.[50] Another part of the statute adds protections against the use of pen registers, which are tools used to monitor the numbers dialed from a person's telephone.[51] Sometimes known

---

43 *Id.* at 157.

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

45 *Id.* at 658-59 (holding that Congress did not intend to protect against intrusions into an individual's email communications under the Wiretap Act).

46 *See* OTA REPORT, *supra* note 35, at 48-52 (analyzing the different stages of the electronic communications process and suggesting various policy options open to Congress in legislating government access to electronic mail).

47 *Id.* at 49-50 (explaining that electronic communications which had been printed out and mailed "would receive the same protections that are accorded first class mail").

48 *Id.* at 50 ("[I]t is possible that an individual would not have a legal basis from which to challenge an electronic mail company's disclosure of the contents of messages or records of messages sent.").

49 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

50 This amendment was Title I of ECPA, and it amended 18 U.S.C. §§ 2510-22 (2006).

51 This amendment was Title III of ECPA, and it was codified at 18 U.S.C. §§ 3121-27 (2006).

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 obtains a court order or the phone company records the numbers for business purposes.[52]

But the most complex part of the new statute, and the part that has become by far the most important, is the section known as the Stored Communications Act (SCA).[53] The SCA creates statutory privacy rights for "subscribers or customers" of two kinds of Internet services.[54] The first kind of Internet service protected by the statute is the one most relevant to individual users. The statute creates privacy protections in email services, referred to in the statute as "electronic communications service" (ECS) providers.[55] 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.[56] 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).[57]

The statute then creates two kinds of protections for customers of the two covered providers. First, it creates legal rules for when the government can compel providers to disclose records about customers and subscribers; second, it creates legal rules for when the providers can disclose records voluntarily.[58] 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.[59] To put the point in language from the Fourth Amendment context, the statute imposes no limits on particularity: there is no need to be specific as to which emails,

---

52 *Id.* For a helpful discussion of the Pen Register Statute, see *In re* Order Authorizing Installation of Pen Register, 846 F. Supp. 1555, 1558-61 (M.D. Fla. 1994).

53 The Stored Communications Act was enacted as Title II of ECPA, and it is codified at 18 U.S.C. §§ 2701-11 (2006).

54 18 U.S.C. § 2702 (2006).

55 18 U.S.C. § 2702(a)(1) (2006).

56 S. REP. NO. 99-541, at 10-11 (1986).

57 18 U.S.C. § 2702(a)(2) (2006).

58 In the current version of the statute, the rules on compelled disclosure are found in 18 U.S.C. § 2703, while the rules on voluntary disclosure are found in 18 U.S.C. § 2702.

59 *See* 18 U.S.C. § 2702(c) (2006) (allowing a provider to "divulge a record or other information pertaining to a subscriber").

which files, or which records were obtained. Instead, disclosure of one record allows disclosure of all records.[60]

Unlike the Wiretap Act of 1968, the SCA of 1986 is notable for imposing no minimization requirement.[61] 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.[62] 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.[63] The government is then free to look through all of it, with no limits on the government's power to use communications it finds, whether relevant or not to the crime under investigation.[64]

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 are noncontent records known as metadata or envelope information.[65] In the context of Internet communications, the contents include the actual messages in emails, together with their subject lines, as well as the contents of files stored on the network.[66] In contrast, the metadata includes IP addresses, to– from information on emails, login times, and locations.[67] As enacted in its original form, the SCA focused its attention on contents held by providers of ECS and RCS instead of noncontent information. Unopened emails stored for less than 180 days received the full protection of a warrant.[68] Opened emails and remotely stored files held by providers of RCS received less protection.[69] But protections for noncontent information were the

---

60 *Id.*

61 *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1298 (2004) (arguing that the SCA along with the Pen Register Act fell short of requiring minimization procedures among other privacy protections).

62 *See, e.g.*, 18 U.S.C. § 2518(6) (2006) (holding that agents may be required to give progress reports to a court).

63 18 U.S.C. § 2702(b) (2006).

64 *Id.*

65 For postal letters, the difference is the letter versus the outside of the envelope.

66 *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611-13 (2003) (discussing the distinction between content and envelope information across different technologies).

67 *Id.* at 614.

68 18 U.S.C. § 2703(a) (1988).

69 *Id.* § 2703(b) (1988).

weakest protections in the statute and appear to be added almost as an afterthought.[70]

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 noncontent information.[71] Under the 1994 Amendment, the government must establish "specific and articulable facts" to obtain a court order requiring the disclosure of many kinds of noncontent Internet records, such as the to–from addresses on emails.[72] This amendment reflects the reasonable suspicion threshold familiar to students of Fourth Amendment law.[73] 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."[74]

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.[75] The 1986 text of the pen register provisions of ECPA was largely telephone-specific.[76] It prohibited the installation of devices to record telephone numbers dialed absent a court order.[77] At the same time, the 1986 text left unclear whether the statute only provided privacy protections for numbers dialed in telephone calls or if the protections also applied to the real-time acquisition of noncontent records relating to Internet communications.[78] 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, or signaling information" relating to any telecommunications network.[79] As a result, the pen register provisions of ECPA now extend to government surveillance of

---

70 *See, e.g.*, 18 U.S.C. § 2703(c) (1988) (highlighting lower requirements for government access to records like payment information, names, and addresses from remote computing services).

71 Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994).

72 *Id.*

73 *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*").

74 *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.").

75 Kerr, *Internetsupra* note 66, at 639.

76 *Id.* at 626.

77 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) (1988).

78 *See* Kerr, *Internetsupra* note 66, at 634 (noting that while the text was unclear, law enforcement practice consistently applied the sections to the Internet).

79 18 U.S.C. § 3127(3) (2006).

noncontent addressing information, such as Internet Protocol addresses and the to–from information for email communications.[80]

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 action based on the statute's distinctions. 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, while 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 noncontent 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, which involves 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.[81] But although the need to update ECPA is widely recognized, existing criticisms of the statute and current reform proposals tend to tinker around the edges of the statute. The proposals retain the basic structure of the statute and only "update" a few sections within it.

Perhaps the best way to appreciate the limited nature of existing criticism is to examine 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.[82] The group includes nonprofit 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.[83]

---

80 *Id.*

81 Savage, *supra* note 4.

82 The corporate members of the group include a virtual "who's who" of the Internet world. *Who We Are*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited Nov. 22, 2013).

83 *Id.*

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.[84] Some background may be helpful to understand this proposal. The SCA imposes a warrant requirement in some cases but not in others. On one hand, the government needs a warrant to compel the release of communications content held by a provider of ECS for up to 180 days.[85] On the other hand, the government does not need a warrant to compel the release of contents held by a provider of ECS for more than 180 days or held by a provider of RCS.[86]

Under this framework, the SCA offers less protection than a warrant to regulate government access to many remotely stored personal files. For example, old emails are no longer fully protected under the ECS rules.[87] Additionally, because individuals often use third party Internet storage services that count under the RCS rules—for example, Google Drive[88] 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

---

84 The Coalition's website explains this proposal in detail:

> 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.

Our Principles, DIGITAL DUE PROCESS COALITION, http://digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Nov. 22, 2013).

85 18 U.S.C. § 2703(a) (2006).

86 *Id.* § 2703(b).

87 This may be true for two reasons. First, the email 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 email 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. Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012).

88 *See generally About Google Drive*, GOOGLE, http://www.google.com/drive/about.html (last visited Nov. 22, 2013).

for mobile devices such as cellular phones.[89] 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; however, the statute did not include any special rules to govern access to records relating to their use. Instead, the current statute treats mobile location information like other noncontent records. Under the SCA, retrospective government access to stored location information generally requires a 2703(d) order.[90] However, because ECPA does not provide for prospective access to location information,[91] the government generally must obtain a warrant under the Federal Rules of Criminal Procedure to obtain ongoing access in "real-time" to such location information.[92] 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.[93] Under the pen register provisions of ECPA, the government can obtain an order to collect noncontent addressing information in real-time with a mere certification that the information to be collected is believed to be relevant to an ongoing investigation.[94] No showing of reasonable suspicion or probable cause is required, and the judge

---

89 *See Our Principles*, *supra* note 84. ("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.").

90 18 U.S.C. § 2703(c) (2006 & Supp. V 2012).

91 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) (2006) ("[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), such call-identifying information shall not include any information that may disclose the physical location of the subscriber.").

92 Lower courts are not uniform on this point, but it is the majority view and, in my view, the correct one. *See generally In re* Application of U.S. For & Order: (1) Authorizing the Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; and (3) Authorizing Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 577-78 (W.D. Tex. 2010).

93 According to the group's proposal,

> A governmental entity may access, or may require a covered entity to provide, prospectively or in real-timereal-timereal-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).

Our Principles, *supra* note 84.

94 18 U.S.C. § 3122(2)(b)(2) (2006).

does not make an independent determination of the facts. The Coalition proposal would require that the government "at least" satisfies the reasonable suspicion standard of a 2703(d) order prior to compelling pen register information.

The final Coalition proposal would limit the government's power to subpoena account information for multiple individuals or accounts.[95] 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.[96] 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 Congressional bills. Nevertheless, it is striking how much the Coalition's 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 noncontent, 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.[97] But whether one agrees or disagrees with them, the existing proposals work within ECPA's outdated framework. The remainder of this Article takes a different approach. Instead of asking how existing laws might be amended, it imagines what Congress should do if it were to start from scratch. Internet technology and Fourth Amendment law is far from where they were in the

---

95 *See Our Principles*, *supra* note 84 ("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.").

96 18 U.S.C. § 2703(c)(2) (2006 & Supp. V 2012).

97 For example, I advocated the Coalition's third proposal in a 2003 article. *See* Kerr, *Internetsupra* note 66, 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 Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 33-42 (2010) (Statement of Orin S. Kerr) (highlighting some of the criticisms of the Coalition's principles presented in this Article).

1980s, and those changes suggest that starting with a clean slate would bring Congress to enact a very different statute. The next Part shows why.

II. HOW CHANGING LAW AND TECHNOLOGY RENDER ECPA OUTDATED

This Section explains how current technology and constitutional law have rendered the dichotomies of ECPA outdated. 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 noncontent. Others are implicit in the statute, such as the territorial scope of the statute and the 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 and providers 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 U.S.-based Internet services serving a predominantly foreign customer base. Additionally, 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 Part 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 SCA. 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. Additionally, 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.[98] 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 than stored access.

That distinction made sense when Congress enacted ECPA. In the 1980s, remote computer storage was very expensive.[99] Internet services of that time were designed to limit storage. After a user read his email from a server, for example, the email typically was downloaded to the user's computer and deleted from the server to save space.[100] Back when remote storage was expensive, the difference between real time and stored access was important. Few sent communications were 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.[101] The government had to carefully limit what information it accessed and then limit what it disclosed. No similar protections were written into the SCA.[102]

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 ten roughly every four years for the last thirty years.[103] The cost of storing a single gigabyte of data has dropped from about eighty-five thousand dollars in 1984 to about five cents in 2011.[104] As the cost of storage drops, Internet services offer the capacity to store everything cheaply. Storage has become the norm. And as storage has become cheap, the norm among users has changed along with it. Users no longer need to be careful about what they keep on the server. The server can keep everything.

---

98 388 U.S. 41, 59 (1967).

99 *See* R.J.T. Morris & B.J. Truskowsi, *The Evolution of Storage Systems*, 42 IBM SYS. J. 205, 205-06 (2003) (examining the evolution of data storage systems and their costs).

100 *See* OTA REPORT, *supra* note 35, at 47 (noting that emails sent over teletext could be saved or deleted by the receiving terminal after they had been viewed).

101 *See* 18 U.S.C. §§ 2510-22 (2006) (extending the minimization requirements of the Wiretap Act from telephone to data transmissions).

102 Solove, *supra* note 61, at 1298.

103 John Villasenor, *Recording Everything: Digital Storage as an Enabler of Authoritarian Governments*, BROOKINGS INST. 3 (Dec. 14, 2011), http://www.brookings.edu/~/media/research/files/papers/2011/12/14%20digital%20storage%20villasenor/1214_digital_storage_villasenor.pdf.

104 *Id.; see also* Morris & Truskowsi, *supra* note 99, at 206 (noting that since 1997 raw storage prices have been declining at 50-60% per year).

To appreciate the difference, consider the storage space available to users of free web-based email services. When free email services became popular in the mid to late 1990s, they generally came with about 2 megabytes of storage space.[105] In contrast, today's popular free Gmail service comes with fifteen *gigabytes* (GB) of storage space, about seventy-five hundred times more storage than was common a decade ago.[106] And it is taken for granted that the space that comes with free email services will only continue to increase.[107]

Many readers will appreciate how the difference has changed their approach to email 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 seventeen thousand emails in her account at any given time.[108] Almost twelve thousand of those emails are received and stored in the inbox; almost six thousand are sent emails directed elsewhere.[109]

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.[110] Among the documents was a report the police had obtained from Facebook containing the stored contents of Markoff's Facebook account. The 72-page

---

105 *See* Paul Festa, *Google to Offer Gigabyte of Free Email*, CNET NEWS (Apr. 1, 2004), http://news.cnet.com/2100-1032-5182805.html (highlighting how Gmail's jump to one gigabyte of storage dwarfed previous storage limits of email providers).

106 Nathan Ingraham, *Google Unifies Gmail, Drive, and Photo Storage: All Users Now Get 15GB of Shared Space*, VERGE (May 13, 2013), http://www.theverge.com/2013/5/13/4326994/google-unifies-gmail-photo-and-drive-storage.

107 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*, VERGE (Apr. 24, 2012), http://www.theverge.com/2012/4/24/2971885/gmail-bumps-free-storage-to-10gb (reporting on the increase to 10GB and predicting that, "as always," the amount of free storage will continue to "creep up over time").

108 Mike Barton, *How Much Is Your Gmail Account Worth?*, WIRED (July 25, 2012), http://www.wired.com/insights/2012/07/gmail-account-worth.

109 *Id.*

110 *See* Carly Carioli, *When the Cops Subpoena Your Facebook Information, Here's What Facebook Sends the Cops*, PHOENIX (Apr. 6, 2012), http://blog.thephoenix.com/blogs/phlog/archive/2012/04/06/when-police-subpoena-your-facebook-information-heres-what-facebook-sends-cops.aspx (noting, among other things, how Facebook reveals little of its involvement in subpoenas from investigators or how many the site serves).

report contained more than just the messages, friends lists, and pictures that we might think of as the contents of a Facebook account.[111] It also contained every comment Markoff had posted and all of the deleted pictures and deleted friends he once had but then tried to erase. 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.[112] 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.[113] 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 is even more revealing and invasive. 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, one time 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 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.[114] In 2012, a total of 633 federal wiretap

---

111 *See Subpoena: Philip Markoff's Facebook Account*, SCRIBD, http://www.scribd.com/fullscreen/88465177?access_key=key-247mvzrfrh1m1azdsoai (last visited Nov. 22, 2013).

112 Carioli, *supra* note 110.

113 *See* Samantha Felix, *This Is How Facebook Is Tracking Your Internet Activity*, BUS. INSIDER (Sept. 9, 2012), http://www.businessinsider.com/this-is-how-facebook-is-tracking-your-Internet-activity-2012-9?op=1 (noting how Facebook uses cookies to both track users and store their information).

114 *See* ADMINISTRATIVE OFFICE OF THE U.S. COURTS, *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the*

orders were obtained.[115] 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"—a category that includes computer communications, pagers, and fax machines—was three.[116] That's not a typo. In the entire United States, federal investigators obtained only three Title III orders to obtain Internet communications.[117]

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 1896 search warrants for accounts operated by Google (most of which were for the contents of Gmail accounts).[118] In light of current trends, this would mean that Google likely received about 4000 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 email accounts in the United States are hosted by Google.

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.[119] In addition, the investigative focus on stored communications partially reflects the lower statutory threshold for access to stored communications. A

Interception of Wire, Oral, or Electronic Communication, (2013), *available at* http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx (providing the annual report online).

115 *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communication*, ADMIN. OFFICE OF THE U.S. COURTS, at tbl.6 (June 2013), http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2012/Table6.pdf.

116 *Id.*

117 Another federal order was obtained 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. *Id.*

118 *Transparency Report: United States*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US (last visited Nov. 22, 2013).

119 *See* Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud* 7 (Ctr. for Interdisciplinary Law & Policy Studies at the Moritz College of Law, Working Paper No. 175, 2012), *available at* http://papers.ssrn.com/id=2038871 (noting that logistical and technical issues are driving the emphasis on stored communication).

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.[120] 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 generally produces the same level of detail as real-time surveillance. As a result, technological change has reversed the assumptions of the 1986 statute.

B. *ECS Versus 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.[121] The ECS protections covered email; the RCS protections covered contents of communications transmitted for remote storage and processing by 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.[122]

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 there was no web to search; the World Wide Web had not yet been invented.[123] Today, however, we send our most private thoughts to Google and other search engines to explore our questions, hopes, fears, and dreams. According to one study, search engines analyzed about 18.4 billion search requests from the United States in March of 2012 alone.[124] That is 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

---

120 *See id.* (indicating the trend of increasing numbers over time).

121 *See supra* Section I.B.

122 *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004) (outlining areas of coverage limitation for the SCA).

123 Tim Berners-Lee invented the World Wide Web in 1990, and the first browser was introduced in 1994. *See* TIM BERNERS-LEE & MARK FISCHETTI, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB 69 (1999); *see also* NICHOLAS CARR, THE BIG SWITCH: REWIRING THE WORLD, FROM EDISON TO GOOGLE 17 (2008) (describing the introduction of the mosaic browser and the intention of gearing toward maximizing the number of users).

124 *See, e.g.*, *ComScore Releases March 2012 U.S. Search Engine Rankings*, COMSCORE (Apr. 11, 2012), http://www.comscore.com/Insights/Press_Releases/2012/4/comScore_Releases_March_2012_U.S._Search_Engine_Rankings (displaying the total searches in February and March of 2012).

months or even years. For example, Google presently stores search queries for 18 months, and previously stored them for 24 months.[125]

ECPA likely offers no protection for access to stored search queries, however, because it does not fit the 1986 dichotomies codified by the statute. Search engines plainly do not provide ECS as they are destinations for communications, not providers of connectivity or messaging.[126] And search queries do not appear to be protected under the RCS rules either. A remote computing service is defined as a service that provides the public "computer storage or processing services by means of an electronic communications system."[127] Users do not send their search queries to Google in order for the site to store them. Storage is a bug for users, not a feature.

The question of whether ECPA protects search queries therefore hinges on whether search engines "process" data that users send them. The relevant text and legislative history suggests that they do not. In the context of computer data, the word "process" suggests performing operations on that data rather than responding 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.[128] Search engines do not seem to fit that mold. Individuals do not use search engines as substitutes for the storage or processing powers of their own machines. Although the issue is difficult and not free from

---

125 Thomas Crampton, *Google to Cut Back on How Long It Keeps Search History*, N.Y. TIMES (June 12, 2007), http://www.nytimes.com/2007/06/12/business/worldbusiness/12iht-google.4.6113031.html?_r=0.

126 18 U.S.C. § 2510(15) (2006) 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.

127 *Id.* § 2711(2).

128 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 in-house on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing. 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, 10-11 (1986).

doubt,[129] it appears likely that the most private of today's communications receive no statutory protection from ECPA.

A second problem with the ECS–RCS dichotomy is that today's Internet services are routinely multifunctional. In 1986, users accessed the Internet by connecting to mainframe computers that gave users access to the network and an email account.[130] In the language of ECPA, they were ECS providers that gave users access to services that included RCS providers. Today, however, users connect to the Internet in many different ways, including broadband and wireless accounts. Network access is always present, running in the background rather than acting as a conscious user destination.[131] At the same time, content messaging such as email or text messaging is simply one service available among many bundled together. Take the example of Facebook.[132] Facebook is not just an email service. Rather, Facebook offers an amalgam of many different kinds of services, including email, chat, photograph hosting, search functions, and bulletin board services.

The multifunctional nature of modern Internet services creates headaches for ECPA by raising complex and perhaps unanswerable questions about what the statute protects. ECPA's privacy protections hinge on the status of the provider. Given that providers wear multiple hats, multiple privacy protections may apply to records. Imagine that a provider acts as an ECS for one set of communications, an RCS for another, and neither an ECS nor an RCS for a third. What privacy protections should apply when the government seeks the disclosure of records under the statute? If the government is seeking noncontent records, the current statute offers

---

129 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 argued 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 remote computer facilities of Google to process and store their search requests and to retrieve by elec-electronic transmission their search results.

Google's Opp'n to the Gov't's Motion to Compel at 12, Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 06-80006), 2006 WL 543697, at *12 (citation omitted).

130 It was also during this time that personal computers began to make gains on the mainframe-computing model. *See* CARR, *supra* note 1233, at 54-55 (describing the increased acceptance of the personal computer as a business tool).

131 *See* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1314 (2012) (describing the "always on" nature of modern communications devices).

132 *See* FACEBOOK, http://facebook.com. As if any cite were necessary.

conflicting answers depending on what service are provided for those sets of records.[133] The old dichotomies don't fit today's technological practices.

C. *Content Versus Noncontent Metadata*

The next dichotomy in ECPA is the distinction between the contents of communications and noncontent 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.[134] Statutory protections guaranteed privacy if the Fourth Amendment protections did not materialize or at least until they did so. In contrast, ECPA's protections for noncontent information were an afterthought.[135] Although later amendments paid more attention to privacy concerns in noncontent 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 fundamental,[136] but metadata analysis has become a more powerful tool than before. Metadata analysis has also

---

133 For example, imagine a company employee logs into the company server to write an email 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 email provider—that is, as a provider of ECS—then it needs a 2703(d) order to compel the noncontent 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 does not apply at all: The provider is not an ECS because it is not providing email service with respect to that file and cannot be a provider of RCS because its services are not available to the public. Whether the statute applies depends on the metaphysical question of whether you see the records as relating to the email or the stored file.

134 *See* OTA REPORT, *supra* note 35, at 3 (noting that the Fourth Amendment's protections have not kept pace with technological advances). 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's adoption. 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.

135 *See supra* Part I.C.

136 *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1019-22, 1034-35 (2010) ("To apply the Fourth Amendment to the Internet in a technologically neutral way, access to the contents of communications should be treated like access to evidence located inside. . . . [and] access to noncontent information should be treated like access to evidence found outside.").

become comparatively important with the rise of encryption.[137] Internet services that generate metadata possess it in unencrypted form. Encryption that might complicate or entirely thwart content surveillance may still leave metadata available for government analysis.[138]

Second, changing law may render the content protections of ECPA much less important. In the last few years, several lower courts have ruled that the Fourth Amendment fully protects the contents of emails held by third party providers. The leading case is *United States v. Warshak*, a Sixth Circuit decision by Judge Boggs involving government access to emails held by the defendant's Internet service provider.[139] Investigators relied on a provision of the SCA to subpoena the defendant's Internet service provider for the contents of stored emails relating to a massive fraud scheme.[140] The provider complied and gave investigators copies of thousands of email messages without a warrant. The Sixth Circuit held that obtaining the contents of emails without a warrant was unconstitutional: users have a reasonable expectation of privacy in their emails just like their letters and phone calls.[141] As a result, the provision of the SCA permitting the government to obtain emails with less process than a warrant was unconstitutional.[142]

Several courts have agreed with the Sixth Circuit since *Warshak*, including federal courts in Kansas[143] and the District of Columbia,[144] and the state of Washington Court of Appeals.[145] Other courts have applied *Warshak* to

---

137 *See generally* Swire, *supra* note 119 (connecting technology changes to changes in surveillance practices).

138 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* Kerr, *Internetsupra* note 66, at 646 n.190 (describing the confusion surrounding whether certain metadata constitutes "content" or "addressing information" for Fourth Amendment purposes).

139 631 F.3d 266 (6th Cir. 2010).

140 *Id.* at 281-83.

141 *Id.* at 285-86.

142 *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.").

143 *In re* Applications for Search Warrants for Info. Associated with Target Email Address, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) ("The Court finds the 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 through an electronic communications service provider.").

144 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).

145 *See* State v. Hinton, 280 P.3d 476, 483 (Wash. Ct. App. 2012) ("While *Warshak* does not aid Hinton, its comparison of emails 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.").

find a reasonable expectation of privacy in stored Facebook messages,[146] text messages,[147] faxes,[148] and password-protected websites.[149] Moreover, multiple courts have presumed Fourth Amendment protection in emails. In evaluating the lawfulness of warrants obtained to collect emails pursuant to Section 2703(a) of ECPA, those courts have mostly not even paused to consider whether the communications might be unprotected.[150] 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, as 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 emails.

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's role can change. Statutory protections are still needed to regulate nongovernmental access to contents of communications that the Fourth Amendment will not reach.[151] But recent Fourth Amendment rulings suggest that the focus of the statute can turn more to noncontent information, such as logs and IP addresses that remain outside the Fourth Amendment.[152]

Granted, the constitutional protections remain tentative and the Supreme Court has not yet spoken. There is significant value in statutory

---

146 R.S. *ex rel.* S.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) ("The Court agrees that one cannot distinguish a password-protected private Facebook message from other forms of private electronic correspondence.").

147 *See Hinton*, 280 P.3d at 483.email

148 *In re Applications for Search Warrants*, 2012 WL 4383917, at *5.

149 United States v. D'Andrea, 497 F. Supp. 2d 117, 121-22 (D. Mass. 2007).

150 *See, e.g.*, United States v. Bowen, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010); United States v. Cioffi, 668 F.Supp.2d 385, 396 (E.D.N.Y. 2009); United States v. McDarrah, 2006 WL 1997638, at *9-10 (S.D.N.Y. July 17, 2006), *aff'd*, 351 F. App'x 558 (2d Cir. 2009). *But see In re Applications for Search Warrants*, 2012 WL 4383917, at *3-5 (discussing the Fourth Amendment question).

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

152 *See* United States v. Forrester, 512 F.3d 500, 510-11 (9th Cir. 2008) (holding that noncontent information such as IP addresses and the to–from information of email addresses is not protected by the Fourth Amendment).

protections before the constitutional precedents are clearly established.[153] At the same time, another constitutional development handed down after ECPA renders its content protections a mixed bag. In *Illinois v. Krull*, the Supreme Court held that the exclusionary rule does not apply when the police conduct a search in reasonable reliance on statutory authority.[154] An Illinois state statute allowed the police to conduct warrantless inspections of automobile salvage yard records.[155] After the Illinois Supreme Court ruled the searches pursuant to the statute unconstitutional, the U.S. Supreme Court held that the exclusionary rule nonetheless did not apply because the officers had reasonably relied on the statute authorizing warrantless searches.[156]

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 without resolving how the Fourth Amendment applies. That largely explains why the *Warshak* Court is the only federal circuit court to date that has directly addressed Fourth Amendment protections in email. Litigation over Fourth Amendment rights in email rarely reach the merits in light of *Krull*.[157] Eliminating content protections under ECPA may paradoxically speed up the process of establishing the apparent strong constitutional protections.

D. *Particularity and Minimization of Internet Communications and Records*

The fourth outdated feature of ECPA is the absence of any reference to particularity or minimization of records obtained beyond the Wiretap Act.

---

153 *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) (discussing the "institutional limitations of judicial rulemaking" and the "significant institutional advantage" of legislatures with respect to the regulation of "criminal investigations involving new technologies").

154 480 U.S. 340, 342 (1987).

155 *Id.* at 343.

156 *Id.* at 355-57.

157 I discussed how the *Krull* good-faith exception has delayed the case law on the Fourth Amendment implications of government access to email 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 (2011).

Particularity is a concept from Fourth Amendment law that refers to the scope of searches and seizures.[158] The Fourth Amendment states that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."[159] By limiting the scope of searches, the particularity requirement helps avoid fishing expeditions. For example, it ensures that searches are directed at a single house rather than a city block (or entire city), and that they aim to collect specific evidence instead of any evidence.

Applying the particularity concept to records collected from Internet providers prompts a difficult question: After the government satisfies the relevant threshold to obtain records, how many records may 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 rare. Companies generally deleted copies of emails read by users to save space for other messages.[160] As a result, Congress never considered how the particularity standard applied to records collected from Internet providers. Investigators could not collect enough records to make particularity an issue, so the statute does not limit the particularity of orders to obtain information.

The absence of any reference to the particularity of court orders creates considerable headaches today. Storage has become cheap, and Internet providers store vast amounts of information by default. As a result, the scope of records which may be obtained has become vitally important. Recall the example of the court order to obtain the contents of a single Facebook account.[161] The 72-page report, which the Boston Police Department had collected pursuant to ECPA to solve the case of the so-called "Craigslist Killer," reflected every single message, photo, and mouse click ever associated with the account.[162] 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 on court orders that seek records regarding hundreds or even thousands of users. A surveillance practice known colloquially

---

158 *See, e.g.*, Maryland v. Garrison, 480 U.S. 79, 84-85 (1987) (stating that the particularity requirement allows only warrants that offer particular and specific descriptions of places that are to be searched).

159 U.S. CONST. AMEND. IV.

160 *See generally supra* Section I.B.

161 *See supra* notes 42-44.

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

as a "cell tower dump" illustrates the problem.[163] Cell phones must maintain contact with local cellular towers to route communications between the phones and the phone network.[164] As a result, cell phone companies generate records showing which phones are in communication with particular towers at specific times.[165] This so-called "cell-site" data provides a rough indication of the location of the phone, and thus presumably the location of its owner. A "cell tower dump" refers to the practice of obtaining records of all customers whose phones were in contact with a cell tower or group of towers over a particular period of time when a crime occurred.[166] For example, if a bank robbery occurred on Main Street at 3 PM, a cell tower dump might allow the government to obtain records of every cell phone user whose phone was in contact with towers near Main Street at that time.

In its current form, ECPA says nothing about the particularity of cell tower dumps. The statutory text merely states 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."[167] 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 ECPA allows court orders for multiple customers—as courts so far have assumed—then the statute is remarkably tone deaf to the scale of the privacy invasion.

To see why, imagine a case where the police believe a house was robbed between noon and 6 PM on a busy city block. Does ECPA allow the police to obtain records for the entire six-hour window, potentially implicating thousands of users? And how many towers can the records concern? And what may the government do with all the data that it obtains, very little of which is likely to be relevant to the investigation?[168]

Constitutional doctrine can address the particularity problem in ECPA within the narrow context of contents already protected by Fourth Amendment. In one recent case, a magistrate judge refused to issue a search warrant sought under ECPA for the contents of an email account and a fax

---

163 *See, e.g.*, *In re* U.S. *ex rel.* Order Pursuant to 18 U.S.C. § 2703(d), Nos. 12-670, 12-671, 12-672, 12-673, 2012 WL 4717778, at *1 (S.D. Tex. Sept. 26, 2012) (noting how the lack of government protocol on collecting information from cell tower dumps raises privacy issues).

164 *Id.*

165 *Id.*

166 *Id.*

167 18 U.S.C. § 2703(c)(1) (2006).

168 *See In re* U.S. *ex rel.* Order Pursuant to 18 U.S.C. § 2703(d), 2012 WL 4717778, at *4.

account because the requested warrants were insufficiently particular.[169] The warrant applications asked for "all records and other information regarding the account"[170] 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."[171]

The Magistrate Judge held that such a request for information was "too broad and too general"[172] to satisfy the Fourth Amendment. A warrant for the entire contents of the account was akin "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."[173] Because the Fourth Amendment would not permit such a warrant for the post office, it would not "permit a similarly overly broad warrant just because the information sought is electronic communications versus paper ones."[174]

Although the Fourth Amendment particularity requirement can address the scope of searches for contents, it cannot serve the same role for noncontent information that is outside the scope of constitutional protection.[175] 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 aspect of ECPA is its territorial scope. In 1986, when the statute was drafted, communication over computer networks occurred mostly in the United States. Commercial providers such as CompuServe provided U.S. users with email and bulletin board services reachable by telephone and modem with U.S. numbers, but international calling rates made such services all but inaccessible outside the United States.[176] The

169 *In re* Applications for Search Warrants for Info. Associated with Target Email Address, 2012 WL 4383917, at *10-11 (D. Kan. Sept. 21, 2012).

170 *Id.* at *8.

171 *Id.* at *9.

172 *Id.* at *8.

173 *Id.* at *9.

174 *Id.*

175 *See* United States v. Forrester, 512 F.3d 500, 510-11 (9th Cir. 2008) (holding that the Fourth Amendment does not protect noncontent information such as IP addresses and the to–from information of email addresses).

176 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.

U.S. government had established ARPANET, which eventually morphed into the Internet,[177] but its use was heavily oriented toward users located in the United States.[178] As a result, issues regarding the territorial scope of the statute did not arise in early debates over ECPA. Congress was instead focused on the rights of U.S. computer users and U.S. services.

Even today, surprisingly few court decisions have addressed the current territorial scope of ECPA. Most of the relevant precedents involve the scope of the Wiretap Act. Courts have held that the telephone wiretapping provisions of the Wiretap Act only apply to interceptions inside the United States.[179] 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."[180] The second ground is that the Wiretap Act provides only for U.S. courts issuing wiretap orders in their jurisdictions, which suggests that Congress intended to limit the territorial scope of the Act to the United States.[181] As a result, the Wiretap Act does not regulate any interceptions occurring outside U.S. 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.*[182] 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.[183] The district court rejected plaintiffs' claim that the disclosure violated ECPA on the ground that ECPA does not apply to disclosures outside the United States.[184] In reaching

177 *See* Reno v. ACLU, 521 U.S. 844, 849-50 (1997).

178 By the time *Reno* went to trial, sixty percent of Internet servers were located in the United States. *Id.* at 850.

179 *See* United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987) (holding that the Wiretap Act "has no extraterritorial force"); U.S. v. Toscanino, 500 F.2d 267, 279-80 (2d Cir. 1974) (finding that the "federal statute governing wiretapping and eavesdropping has no application outside the United States" (citation omitted)).

180 United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975).

181 *Id.* As noted by the district court in *United States v. Angulo-Hurtado*,

> 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.

165 F. Supp. 2d 1363, 1369 (N.D. Ga. 2001).

182 No. 08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009).

183 *Id.* at *1.

184 *Id.* at *4.

its decision, the court relied heavily on the reasoning of the cases interpreting the territoriality of the Wiretap Act.[185] It also noted that the enactment of ECPA did not contain any provisions rejecting that traditional territorial scope.[186]

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 access a website across the world as easily 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.[187] Or at least that is the case today, as 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, the popular email service provided by Google. Google is headquartered in California, but only 30 percent of Gmail's users reside in the United States.[188] This chart shows the percentage of Gmail's users that are in a handful of different countries as of September 2013[189]:

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

186 *See Zhang*, 2009 WL 4430297, at *3 ("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 ECPA, in amending the Wiretap Act and creating the SCA, reference in any manner activities occurring outside the United States.").

187 *See '60 Minutes' Report: How Online Gamblers Unmasked Cheaters*, CNET.COM (Nov. 30, 2008), http://news.cnet.com/60-minutes-report-how-online-gamblers-unmasked-cheaters (reporting that members of the Mohawk Kahnawake nation register and service "more than 60% of the world's Internet gaming activity").

188 *Gmail Usage Per Country*, APPAPPEAL.COM, http://www.appappeal.com/maps/gmail (last visited Nov. 22, 2013).

189 *See id.*

Country	Percentage of Gmail Users
United States	30.0%
India	8.8%
Brazil	3.3%
Russia	3.2%
United Kingdom	2.9%
Japan	2.6%
Iran	2.4%
China	1.4%

Facebook's user base is even more foreign than Gmail's. To be sure, using Facebook has become as American as apple pie: about 54 percent of Americans presently have a Facebook account.[190] At the same time, only about 16 percent of Facebook's users are located in the United States.[191] The rest access Facebook from abroad. For U.S.-based services like Gmail and Facebook, U.S. users form only a small subset of its overall 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 third country; and the party seeking access to the company's data could be located in a fourth country. Of course, all of the data could be easily sent electronically from any place in the world to any other place. So what determines territoriality? The location of the data? The company? The employee? Or the requesting party?[192] Imagine a person in Mexico who seeks the emails 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

190 Quentin Fottrell, *Facebook Loses 1.4 Million Active Users in U.S.*, MARKETWATCH (Jan. 15, 2013), http://articles.marketwatch.com/2013-01-15/finance/36346107_1_active-users-facebook-social-media.

191 *Id.* (reporting that about 167 million of Facebook's one billion users are located in the United States as of January 2013).

192 Courts have encountered similar questions while 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) (holding that a judge in Wisconsin was statutorily authorized to order a wiretap on a cellular phone regardless of whether the phone or listening post was located in Wisconsin).

servers in the United States. If the company discloses the records, is that disclosure inside the United States for purposes of ECPA? Does it matter if the French employees first have the data emailed 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 email files could be fragmented and the underlying data located in many places around the world.[193] The emails 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 emails 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.*,[194] the location of the customer or subscriber has no bearing on that individual's ECPA rights.[195] Individuals outside the United States who use Gmail from abroad have the same statutory rights as U.S. 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 U.S.-based provider Yahoo! for its failure to disclose records sought about customers in the Netherlands whom Belgian prosecutors suspected of criminal activity.[196] Yahoo!'s

---

193 Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CON. L. HEIGHT. SCRUTINY 11, 20-21 (2012) ("Google Docs or Amazon's cloud-based simple storage service . . . might sometimes choose to store multiple copies of a document, or to partition a single copy of the document into separately stored fragments.").

194 671 F.3d 726, 729 (9th Cir. 2011) ("[T]he plain language of ECPA extends its protections to noncitizens. The Court is therefore obligated to enforce the statute as written.").

195 *Id.* at 729-30.

196 Tanguy Van Overstraeten & Ronan Tigner, *Belgium–Yahoo! Saga Continues: Yahoo! Must Not Hand Over Personal Data to the Public Prosecutor*, LINKLATERS (Jan. 30, 2012), http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-Newsletter-January-2012/Pages/9_Belgium-Yahoo!-saga-continues-Yahoo-personal-data-public-prosecutor.aspx (last visited Nov. 22, 2013).

defense was based in part on ECPA. According to Yahoo!, it was a U.S. provider governed by U.S. law. The criminal case against Yahoo! is still pending in the Belgian courts,[197] 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 U.S.-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,"[198] thus excluding foreign governments. This means that foreign governments cannot obtain mandatory process using foreign court orders.[199] 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.[200] At the same time, because ECPA permits providers to disclose noncontent information to nongovernment entities,[201] providers can disclose noncontent information to foreign governments at their discretion. As a practical matter, then, foreign governments can often obtain noncontent 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 though the order is not binding in the United States.

The picture is more complicated when foreign governments seek content information. Four basic options exist. The first option is for foreign governments to work with the U.S. government and to use Mutual Legal Assistance Treaties or letters rogatory to seek information from providers using official diplomatic channels.[202] This process generally remains slow and laborious, as it requires the cooperation of two governments and one of those governments may not prioritize the case as highly as the other.[203]

A second option is for foreign governments to persuade U.S. officials to open a domestic investigation and obtain U.S. court orders that are binding

---

197 *Id.*

198 *See* 18 U.S.C. § 2711(4) (2006).

199 *See id.* § 2703 (providing means of compelling information for government entities).

200 *See id.* § 2702(a)–(b) (drawing no distinction between private entities and foreign governments for purposes of limiting the voluntary disclosures of customer communications by providers).

201 *See id.* § 2702(c)(6) (permitting disclosure of noncontent information "to any person other than a governmental entity").

202 *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).

203 *Id.*

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 U.S. offense.[204] Further, it requires U.S. 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 use of U.S. resources.

The third option is that a provider could design the network so that a copy of the communication exists outside the United States where ECPA does not apply. For example, the provider could create a policy by which users who register their accounts from outside the United States have copies of their accounts stored outside the United States as a matter of course. If foreign governments approach the provider seeking to obtain the communications, the copy will already exist outside the United States. It seems likely that ECPA would not apply, and the communication can be accessed under the laws of the country in which the copy is retained.

The fourth option is legally dubious but nonetheless worth mentioning: a provider might store the communications in the United States and then export the data to a representative or an affiliate outside the United States when foreign legal process is served. 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 emailing it to a corporate representative abroad. There are no decisions on the issue, however, and the distinction between designing a network so that copies are abroad to facilitate legal process and simply sending a copy abroad in response to legal process is a tricky one. ECPA simply was not written with the territoriality problem in mind.

---

204 Notably, U.S. criminal laws have been expanded extraterritorially to enable U.S. assistance to foreign governments. By making a foreign crime also 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*, CYBERCRIME.GOV (Nov. 5, 2001), http://web.archive.org/web/20011204213823/ (discussing the extraterritorial expansion of the Computer Fraud and Abuse Act as a way to assist foreign computer crime investigations).

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 Part argues that a new privacy statute should be based on four principles. First, Congress should impose 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 noncontent information. Third, Congress should impose minimization rules on all contents of communications obtained by investigators. And fourth, Congress should impose a territoriality regime based on the location of the user, such as one that provides full protections for users based in 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 the 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 a single legal standard for access to the contents of data held by or for a customer or subscriber.

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, which is presently covered by the Stored Communications Act. As explained in Part II, the low storage cost 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 on them. Eliminating the distinction between real-time and stored access is also more practical because 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 the court to treat it as "contemporaneous" and therefore analyze it under the Wiretap Act.[205] 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

---

205 *See* LAFAVE, *supra* note 2, at § 4.6(b).

communications should lead to the same protection, regardless of whether the provider acts as an email 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 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 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 harmonized somewhere in the middle. I have argued elsewhere that the Fourth Amendment ordinarily requires a probable cause warrant for government-compelled access to contents,[206] and that the 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.[207] Because this Article is a thought experiment, I will not attempt to answer where the line should be drawn. Wherever the line is drawn, existing technology counsels in favor of a uniform standard for compelled access to contents.

B. *Particularity Requirements for Noncontent Data Should Be Imposed, Perhaps Based on a Concept of Customer-hours*

The second principle of the new statute should be the adoption of particularity requirements. Outside of the Wiretap Act, ECPA pays no attention to particularity because few records existed that could be collected when the statute was enacted. The amount 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 question of how much cause the government must demonstrate to obtain information

---

206 *See* Kerr, *Internetsupra* note 136, at 1029-31 (arguing that contents are the online equivalent of real-world "inside" information, and should therefore be covered by the Fourth Amendment).

207 *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 80-84 (2004) (arguing that Internet surveillance should adopt the highly protective standards of the Wiretap Act).

should be followed by 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 noncontent information. In the case of contents, the Constitution already requires the government to satisfy traditional Fourth Amendment particularity concerns.[208] 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 noncontent information, which is not protected by the Fourth Amendment.[209]

Identifying the proper particularity standard for noncontent information is difficult because such records exist in many different forms. Some noncontent records are more sensitive than others. A list of every email address that a person emailed, together with the time each email was sent, 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 or type of records the government may request from a particular user or from a range of users. The question is, what principle should Congress use to limit the scope of noncontent records access? Should it be the overall number of records collected, perhaps with limitations on the 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 noncontent information is the concept of customer-hours. In an environment of widespread and detailed recordkeeping, a helpful way to measure the scope of access to metadata is by identifying the length of time for which a customer used the service. If providers collect everything, the time over which the collection occurs most effectively identifies the scope of the metadata collected. Further, if the government may need the records of multiple users, the invasion of privacy grows with the number of users whose records are collected. Imposing a particularity requirement based on a defined maximum number of customer-hours may provide the best way to limit the scope of noncontent records accessed.

---

208 *See, e.g.*, *In re* Applications for Search Warrants for Info. Associated with Target Email Address, Nos. 12-8119, 12--8191, 2012 WL 4383917, at *4-5 (D. Kan. Sept. 21, 2012) (applying Fourth Amendment protections to emails and faxes). Of course, Congress could enforce a particularity limit that is more restrictive than the constitutional limit.

209 *See supra* Section I.C.

An illustration can help explain how such a particularity requirement would work. Imagine that Congress sets the threshold for access to noncontent records using a standard akin to the existing 2703(d) standard: to obtain a court order for disclosure, the government must present "specific and articulable facts" suggesting that the records disclosed would be "relevant and material to an ongoing criminal investigation."[210] Congress could then impose a particularity limit of a specific number of customer-hours for each court order. 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 noncontent 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 1000 customers. In that case, the particularity limitation of 500 customer-hours would restrict the government's access to 30 minutes of time. If the government sought information from more towers, or chose towers with especially high usage, the government could still obtain the order, but only for an even shorter time window.[211]

C. *Minimization Rules Should Apply to All Obtained Contents of Communications*

The next principle that the new statute should reflect is that minimization principles from the Wiretap Act should apply when accessing all contents. Existing law adopts a bifurcated privacy regime. Under the Wiretap Act, lawful access to communications comes with strings attached.[212] Even after obtaining a lawful wiretap order, agents are required to screen communications ex ante and then carefully limit disclosure ex post.[213] Under the SCA, a court order requires the provider to supply the government with the entire contents of the account. The government is then free to look through all of this material.

This was understandable back when few Internet communications were stored. But in a world of total storage, the absence of legal rules on minimization has become an anomaly. Every collection of contents should impose

---

210 18 U.S.C § 2703(d) (2006).

211 Of course, there could be implementation issues with this standard if the number of individuals involved were unknown or varied considerably over time. Nonetheless, the customer-hours approach offers at least a rough way to impose a particularity requirement.

212 *See supra* Section I.B.

213 *See supra* Section I.B.

the same minimization requirements 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 states:

> 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 non-relevant materials and disseminate to other officials only that information which is relevant to the investigation.[214]

As the Ninth Circuit has recognized, minimization for electronic communications requires filtering.[215] Someone must go through the 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.[216]

---

214 S. REP. NO. 99-541, at 31 (1986).

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

216 I have argued elsewhere that the plain view exception should not apply to digital evidence searches, including searches through contents of communications obtained from third-party providers. *See* Kerr, *Internetsupra* note 136, at 1047-48 ("I would incorporate a proposal I have made in the context of stand-alone computers to eliminate the plain view exception for Internet searches."). I continue to adhere to that view, although I will not repeat the argument here.

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 this 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 U.S.-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 available option is to focus privacy protections on the perceived location of the user. Providers usually have a rough sense of the locations of their customers.[217] 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 location of a user from the IP address used to access the network.[218] The combination of language and IP address gives providers a general sense of the country used to access their network by each customer.[219]

A rule based on the location of the user is far from ideal. Some customers access services from multiple countries.[220] Others access services using anonymized IP addresses, making their location difficult to identify. 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

---

217 *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) (discussing how geolocation tools, which currently use IP addresses, can be used to determine an Internet user's physical location).

218 *See id.* at 594-97 (examining the reliability of IP addresses for geolocation).

219 *See id.* at 597 (explaining that "combinations of methods" yield more accurate results than relying on IP addresses alone).

220 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 U.S.-based service is located in the United States unless the evidence indicates otherwise with some clarity.

global network, the location of data is arbitrary and increasingly unknowable. The location of the company holding data is equally arbitrary and difficult to know, given that multinational companies can have affiliates and branches anywhere. A standard based on perceived user location is problematic, but it seems less problematic than the alternatives.

Moreover, difficulties in identifying location can be addressed through presumptions and standards of proof. For example, the default 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 would 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 that are either based in the United States or that are doing business in the United States would be required to follow U.S. privacy law with respect to their U.S.-based users. That requirement would apply regardless of where information is technically stored. Under my proposal, privacy protections should follow the user instead of the data: all state or federal government access to information about U.S.-based users should comply with U.S. law. So long as a company with a presence in the United States has communications belonging to U.S.-based customers, that company should have to follow U.S. 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 U.S.-based users. Users in the United States would also know that their use of U.S.-based services would receive the full protection of U.S. law.

The second part of the solution would focus on the rights of users based outside of the United States. For those users, the law should allow, but not require, Internet providers to disclose contents and noncontent information pursuant to the foreign legal process in the country associated with the user. If French authorities in France produce a valid court order pertaining to a French user, U.S.-based providers should be permitted to comply with the order. This approach would place some burden on providers that service foreign customers, as it would require them to learn enough about foreign legal process to understand foreign court orders. More importantly, however, 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 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 U.S.-based 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 would allow U.S.-based providers to choose which countries should be deemed sufficiently protective and democratic to have their legal process honored.[221] And because that legal process would only apply to users located in the country where the user is located, the law would both protect U.S.-based 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 the countries in which they are located. Hinging privacy protections on the location of the user would ensure 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 those that presently exist. 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.

---

221 Providers likely would not welcome this choice, as it encourages foreign governments to pressure them to disclose and requires providers to make difficult calls. It may prove difficult for a provider to refuse compliance with court orders in countries where that provider has a business presence.

Whether or not Congress is able to enact a wholesale revision of the privacy laws, it should realize that substantial reform will likely 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 significantly more important to American life. The incredible growth of the Internet and its 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. Today's Internet 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 instead of the past.