The Electronic Communications Privacy Act of 1986: Principles for Reform

J. Beckwith Burr[1]

Background

Congressional enactment of the Electronic Privacy Information Act (ECPA)[2/] in 1986 was a remarkably forward-looking effort to govern the compelled disclosure of electronic communications data to the government by balancing law enforcement needs with the personal privacy safeguards needed in the digital age.[3/] As communications technology developed, and its contribution to the U.S. economy became clear, Congress also consciously endeavored to find a balance that would nurture communications technologies.[4/] The wisdom of this attempt to balance privacy rights and law enforcement needs in an innovation-friendly environment is evident today: the Internet has evolved from a research network with a few thousand academic hosts into a global platform for communications, commerce, and civic activity used by four out of five adults in the United States on a daily basis.[5/] Information technology has driven the U.S.

---

[1] J. Beckwith Burr is a partner at Wilmer Cutler Pickering Hale and Dorr, LLP, and a member of the firm's Regulatory and Government Affairs Department, based in Washington, D.C.

[2/] The term "ECPA" is used in this paper to describe both Title I of the Electronic Communications Privacy Act, which protects wire, oral, and electronic communications in transit, as well as Title II, referred to as the Stored Communications Act, which protects communication held in electronic storage.

[3/] The stated goal of ECPA was to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement." House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2, at 19 (1986).

[4/] In addition to the goals of privacy and law enforcement, ECPA sought to advance the goal of supporting the development and use of these new technologies and services. *See* S. Rep. No. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems"). It was the intent of Congress to encourage the proliferation of new communications technologies, but it recognized that consumers would not trust new technologies if the privacy of those using them was not protected. *Id.*; H.R. Rep. No. 99-647, at 19 (1986).

[5/] Pew Internet & American Life Project: *Wireless Internet Use*, at 8 (July 2009) , *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/Wireless-Internet-Use.pdf

economy in the past two decades,[6/] and is expected to remain the engine of growth for years to come.[7/]

As forward-looking as ECPA was in 1986, there is broad consensus that today's technology has outpaced the Act. In 1983, Apple Computer introduced the "Lisa"—the first mass-marketed microcomputer with a graphical user interface. The Lisa cost $10,000 and featured 1 megabyte of RAM and a 5 megabyte hard drive.[8/] Today, for $999, consumers can purchase a Mac Book with 2 gigabytes of memory, a 250 gigabyte hard drive, and built in wireless Internet access and communications technology.[9/] In 1995—nearly a decade *after* Congress enacted ECPA—only 9% of American adults used the Internet, compared to 81% today.[10/] Prototype mobile telephones from the 1980s—the size and shape of "bricks"—are now

---

[6/] *See* Robert D. Atkinson & Andrew S. McKay, *Information Technology & Innovation Foundation, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 11-14 (March 2007) ("[T]he mid-1990s were a turning point that marked the move from the sluggish U.S. economy of the 1970s, 1980s, and early 1990s to the dynamo of the last decade… [T]here is a now a strong consensus among economists that the IT revolution was and continues to be responsible for the lion's share of the post '95 rebound in productivity growth.").

[7/] *See id*. at 53 ("It is not clear how long IT will power growth, but it seems likely that for a[t] least the next decade or two IT will remain the engine of growth. The opportunities for continued diffusion and growth of the IT system appear to be strong. Many sectors, such as health care, education, and government, have only begun to tap the benefits of IT-driven transformation. Adoption rates of e-commerce for most consumers, while rapid, are still relatively low. And new technologies (*e.g.*, RFID, wireless broadband, voice recognition) keep emerging that will enable new applications. In short, while the emerging digital economy has produced enormous benefits, the best is yet to come. The job of policymakers in developed and developing nations alike, is to ensure that the policies and programs they put in place spur digital transformation so that all their citizens can fully benefit from robust rates of growth.").

According to the Bureau of Labor Statistics, "Two of the fastest growing detailed occupations are in the computer specialist occupational group. Network systems and data communications analysts are projected to be the second-fastest-growing occupation in the economy. Demand for these workers will increase as organizations continue to upgrade their information technology capacity and incorporate the newest technologies. The growing reliance on wireless networks will result in a need for more network systems and data communications analysts as well. Computer applications software engineers also are expected to grow rapidly from 2008 to 2018. Expanding Internet technologies have spurred demand for these workers, who can develop Internet, intranet, and Web applications." *Occupational Outlook Handbook: 2010-2011 Edition, available at* http://www.bls.gov/oco/oco2003.htm.

[8/] Lisa/Lisa 2/Mac XL, *available at* http://www.apple-history.com/lisa.html.

[9/] Apple—MacBook: Technical Specifications, *available at* http://www.apple.com/macbook/specs.html (last visited Feb 2010).

[10/] Harris Interactive, The Harris Poll, *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=973.

collector's items on eBay,[11/] while in 2009 palm-sized smart phones[12/] double as sophisticated computing platforms with the potential to bridge the digital divide.[13/] Communications technology in the United States is evolving—and will continue to evolve—more rapidly and in more directions than we currently imagine. ECPA, which served us remarkably well for many years, is today unwieldy and unreliable as a law enforcement tool, immensely difficult for judges and investigators to apply, confusing, costly, and full of legal uncertainty for communications and other technology tools and service providers, and an unpredictable guardian of our country's long cherished privacy values.

A coalition of communications, equipment, and online services, as well as members of the legal and advocacy communities[14/] have come together over the last year with the goal of developing a set of principles to simplify, clarify, and unify ECPA—without constraining important law enforcement activities. The result of this effort is a set of consensus principles for updating ECPA that are designed to:

- **Establish consistent, predictable privacy protections** for communications and other electronic information services used by Americans every day to handle their personal communications and operate their businesses — building user trust and supporting the full extension of Constitutional values to the networked world, while providing clarity for law enforcement and service providers.

- **Achieve technologically neutral solutions** and avoid arbitrary distinctions that become hard to apply over time, inhibit innovation, and skew the Internet marketplace.

11/ For example, Motorola's Dynatax 8000x was the first cell phone to receive FCC approval (in 1983). It weighed 28 ounces and was 10 inches high, not including its flexible "rubber duck" whip antenna. *Available at* http://www.retrowow.co.uk/retro_collectibles/80s/motorola_8000X.php.

12/ For example, the Google Nexus One is less than 5 inches tall and weighs less than 5 ounces. *Available at* http://www.google.com/phone/static/en_US-nexusone_tech_specs.html.

13/ According to the Pew Internet & American Life Project, lower levels of home broadband access coupled with lower levels of desktop and laptop computers explains the traditional access gap between white and black Americans. But the gap in online engagement "largely dissipates" according to Pew, when access on handheld and mobile devices is considered: under those circumstances, "use among African Americans matches or exceeds that of white Americans. Two measures of engagement with the wireless online—accessing the [I]nternet on a handheld on the typical day or ever—shows that Africans Americans are *70% more likely* to do this than white Americans." The report concludes, "To an extent notably greater than that for whites, wireless access for African Americans serves as a substitute for a missing onramp to the Internet—the home broadband connection." Pew Internet & American Life Project: *Wireless Internet Use*, at 32-35 (July 2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/Wireless-Internet-Use.pdf (emphasis in original).

14/ Coalition members currently include: American Civil Liberties Union, AT&T, Center for Democracy and Technology, Electronic Frontier Foundation, Google, Microsoft, IBM, Net Coalition, Loopt, and Salesforce.com.

- **Preserve the legal tools necessary to conduct criminal investigations and protect the public**, including through preservation of the ECPA exceptions and exemptions relied upon by law enforcement today.

The consensus principles reflect the working group's commitment to *change no more than strictly necessary to achieve these important goals*. Implementation of the consensus principles would not affect surveillance or privacy law relating to national security, including the Foreign Intelligence Surveillance Act and the national security letter authority in ECPA. The principles would not deny the government information needed to conduct investigations, and no information would be rendered off limits to government investigators with appropriate process. Indeed, adoption of the principles would facilitate cooperation between business and law enforcement by clarifying the rules under which the parties interact. The principles preserve all of the building blocks of criminal investigations—subpoenas, court orders, pen register/trap and trace orders, and warrants, and would carry forward ECPA's sliding scale approach that ties the level of process required to the level of investigative intrusiveness. The recommended changes would not disturb fundamental elements of ECPA, including the distinctions between content, subscriber identifying information, and less sensitive transactional data. Finally, these recommendations preserve the exceptions for compelled disclosure that have been written into ECPA over the years, including those permitting emergency disclosures.

Principles

1. 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.

2. 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.

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

4. 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.

Principle 1: Access to Content in Transit and in Storage

Recommended Approach: Under the consensus principles, a governmental entity may require the provider of wire or electronic communications services to produce the non-public content of communications only with a search warrant issued based on a showing of probable cause, regardless of the age of the communication, the means or status of its storage or the provider's access to or use of the content in its business operations. This change would bring all stored communications content under the same probable cause standard set forth in the Fourth Amendment, accessible to law enforcement with an ordinary warrant. For example, a showing of probable cause would be required to compel production of email, regardless of whether it is "opened" or not, and regardless of how old it is. The principle also would apply to documents and other private data stored by or on behalf of individuals on remote servers.[15/]

Need for Change: Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Most people save these emails, just as they previously saved letters and other correspondence.[16/] In fact, many Americans now have accumulated years' worth of email, much of which is stored on the computers of trusted third-party service providers. Likewise, businesses and individuals are

---

15/ These changes are premised on the understanding that the definition of "electronic communications" is broad enough to include such items as a draft document stored on a service such as Google Docs. We interpret the current definition of remote computing service as broad enough that it does not need to be amended to cover technologies such as cloud computing, which are expected to keep America competitive by reducing business costs, enhancing productivity, and facilitating collaboration and innovation.

16/ Companies often impose email retention policies that require employees to preserve emails for several months before deletion. Contoural White Paper, *How Long Should Email Be Saved?*, at 5 (2007), *available at* http://www.umiacs.umd.edu/~oard/teaching/708x/spring09/t1.pdf. ("Most companies come to the conclusion that many messages should be retained for a few years for business productivity purposes.").

Moreover, unlike a paper letter, often an email remains in existence long after the sender or recipient attempts to delete it. *See* Applied Discovery, at 3, *available at* http://www2.acc/chapters/program/dallas/documentretention.pdf. ("Even when a computer user intends to discard electronic data, the task is much easier said than done. The 'delete' key creates a false sense of security for many people. A deleted document may no longer be available to the user, but copies remain in temporary files, on backup tapes, and, in the case of email, in other recipients' in-boxes.")

now increasingly storing other data "in the cloud,"[17/] with huge benefits in terms of productivity, cost, security, flexibility and the ability to work with collaborators around the world.[18/] This data includes highly personal information such as medical and financial data, digital calendars, photographs, diaries, and correspondence.[19/] It also includes commercially sensitive, proprietary and trade secret materials, such as business plans, research and development, and commercial collaboration.

The privacy rights of an individual with respect to all of this information, if stored on his or her hard-drive[20/]—or indeed on a CD in a safe deposit box—would be fully protected by the warrant clause.[21/] Under ECPA, however, a single email or electronic document could be subject to multiple legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient or uploaded into a user's "vault" in the cloud, where it might be subject to an entirely different standard.[22/] A warrant is required to access the content

---

17/ "Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flow charts and diagrams." Cloud Computing Definition, *available at* http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html.

18/ As an example of the potential savings from cloud computing, the Obama Administration's Chief Information Officer, Vivek Kundra, "pointed to a revamping of the General Services Administration's USA.gov site. Using a traditional approach to add scalability and flexibility, he said, it would have taken six months and cost the government $2.5 million a year. But by turning to a cloud computing approach, the upgrade took just a day and cost $800,000 a year." Daniel Terdiman *White House Unveils Cloud Computing Initiative*, cnet News, Sept. 15, 2009, *available at* http://news.cnet.com/8301-13772_3-10353479-52.html

19/ These materials are, as one author has noted, "the same materials deemed 'highly personal' by the Supreme Court, a sentiment later echoed by the Eighth Circuit to justify Fourth Amendment protection for schoolchildren despite their otherwise diminished expectations of privacy. [They] also mirror [ ] the list of materials that the Eleventh Circuit used as a basis for asserting that 'few places outside one's home justify a greater expectation of privacy than does the briefcase.'" *See* David A. Couillard , *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205, 2219-2220 (2009) (internal footnotes omitted).

20/ *See, e.g.*, *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001); *United States v. Crist*, No. 1:07-cr-211, 2008 WL 4682806 (M.D. Pa. Oct. 22, 2008).

21/ See, *e.g.*, *Kyllo v. United States*, 533 U.S. 27, 31 (2001) ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." (internal quotations and citations omitted)).

22/ Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, at 13 (Feb. 23, 2009). "Distinctions recognized by ECPA include electronic mail in transit; electronic mail in storage for less than or more than 180 days; electronic mail in draft; opened vs. unopened electronic mail; electronic communication service; and remote computing service.… The precise characterization of an activity can make a significant difference to the protections afforded under ECPA." *Available at* http://www.scribd.com/doc/12805751/Privacy-in-Cloud-Computing-World-Privacy-Council-Feb-2009.

of an email while it is in storage waiting to be read by the recipient.[23/] The nanosecond the email is opened by the recipient, however, it may lose that high standard of protection and become accessible with a subpoena, issued with no judicial intervention, with (concurrent or delayed) notice to the affected individual.[24/] One Court of Appeals has rejected this distinction between opened and unopened communications for purposes of determining whether or not a communication is in "electronic storage,"[25/] while in other areas of the country the question remains unsettled.[26/] In all cases, the Justice Department believes law enforcement can compel disclosure of the content of the same email with a mere subpoena after the email is more than

---

[23/] 18 U.S.C. § 2703(a).

[24/] 18 U.S.C. § 2703(b)(1)(B). Alternatively, it can be acquired with prior notice to the subscriber based upon a court order supported by specific and articulable facts demonstrating reasonable grounds to believe the communication is relevant to an ongoing criminal investigation. *Id*. In either case, notice to the subscriber is required unless the government secures a warrant. *Id*. The Department of Justice Computer Crimes and Intellectual Property Section argues in the 2009 edition of its Computer Search and Seizure Manual, at 123-124: "As traditionally understood, 'electronic storage' refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity. It does not include post-transmission storage of communications. For example, email that has been received by a recipient's service provider but has not yet been accessed by the recipient is in 'electronic storage.' *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994). At that stage, the communication is stored as a temporary and intermediate measure pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the email, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the accessed communication, the copy will not be in 'temporary, intermediate storage' and is not stored incident to transmission. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) (stating that email in post-transmission storage was not in "temporary, intermediate storage"). By the same reasoning, if the sender of an email maintains a copy of the sent email, the copy will not be in 'electronic storage.' Messages posted to an electronic 'bulletin board' or similar service are also not in 'electronic storage' because the website on which they are posted is the final destination for the information. *See Snow v. DirecTV, Inc*., 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005), *adopted by* 2005 WL 1266435 (M.D. Fla. May 27, 2005), *aff'd on other grounds*, 450 F.3d 1314 (11th Cir. 2006). http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

[25/] *Theofel v. Farey Jones*, 359 F.3d 1066 (9th Cir. 2004).

[26/] The Department of Justice Computer Crimes and Intellectual Property Section Manual describes the holding of the Ninth Circuit in *Theofel* as follows: "[T]he court held that email messages were in 'electronic storage' regardless of whether they had been previously accessed, because it concluded that retrieved email fell within the backup portion of the definition of 'electronic storage.' *Id*. at 1075-1077. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that a previously accessed email message fell within the scope of the 'backup' portion of the definition of 'electronic storage,' because such a message "functions as a 'backup' for the user." *Id.* at 1075. The discomfort of some courts with the Justice Department's interpretation of the Stored Communications Act is evident in the Sixth Circuit's (now vacated) ruling in *Warshak v. United States* that "individuals maintain a reasonable expectation of privacy in emails that are stored with, or sent or received through, a commercial ISP." 532 F.3d 521, 536-537 (6th Cir. 2008). Specifically, the panel court upheld a preliminary injunction enjoining the government from "seizing the contents of a personal e-mail account" under 18 U.S.C. § 2703(d) unless the government provides prior notice to the e-mail user or shows that the e-mail user had no reasonable expectation of privacy vis-à-vis the e-mail service provider.

180 days old.[27/] Likewise, while as a practical matter law enforcement must secure a warrant to access documents on a personal computer, under ECPA, a mere subpoena issued to a third party will suffice to access confidential documents stored remotely on the computers of a cloud computing service provider.[28/]

The different standards are the unanticipated byproduct of technology changes, and not a careful balancing of the needs of law enforcement and the privacy rights of individuals. Nor do they reflect a substantive difference in the nature of the information; rather they reflect the fact that ECPA was enacted in 1986—six years before Congress authorized commercial activity on the Internet,[29/] and seven years before the first web browser was introduced.[30/] In 1986, very few Americans had e-mail accounts, and those who did typically downloaded email from a server onto their hard drives, and email was automatically and regularly overwritten by service providers grappling with storage constraints.[31/] Even eight years later, when Congress enacted the Communications Assistance for Law Enforcement Act (CALEA),[32/] the commercial Internet

---

27/ *See* DOJ, *Electronic Surveillance Manual*, at 25 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

28/ 18 U.S.C. § 2703(b). While the government requires a warrant under Rule 41 to forcefully enter and seize someone's personal computer, it could theoretically choose to use a subpoena to compel production of the same computer or its contents, resorting to court enforcement if the recipient failed to comply with the subpoena. As a practical matter, however, concerns about compromising the investigation or destruction of evidence normally lead law enforcement to secure a warrant in this situation. The same concerns about compromise and loss of evidence are not normally present when the subpoena is served on a third party service or storage provider, however.

29/ Prior to 1992 the National Science Foundation's mandate was to support access to the Internet for research and education, and it had no authority to permit or promote commercial activity on the networks connecting research and academic institutions. This authority was conveyed to the NSF only in 1992, with passage of The Scientific and Advanced-Technology Act, 42 U.S.C. § 1862(g) (1992), which directed the National Science Foundation "to foster and support access by the research and education communities to computer networks which may be used substantially for purposes in addition to research and education in the sciences and engineering, if the additional uses will tend to increase the overall capabilities of the networks to support such research and education activities."

30/ The Mosaic web browser was released in 1993, a graphical browser developed by a team at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign (UIUC), led by Marc Andreessen.

31/ Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. Rev. 1043, 1072 (Note 2008) ("In 1986, e-mail technology was still very new. Most e-mail users dialed-up to their e-mail servers using a modem and downloaded their communications to a home computer, with the server acting only as a medium for temporary storage. Using this rationale, the ECPA draws a distinction between e-mails in electronic storage on third-party servers for 180 days or less and those in electronic storage longer than 180 days." Citing *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 475, at 24 (1986) (testimony of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association)).

32/ Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1021).

was in its infancy, digital storage was expensive,[33/] and email was automatically and regularly overwritten by service providers grappling with storage constraints.

Today, the distinctions between and among data in transit, data in electronic storage, data stored by a remote computing service, and data more them 180 days old no longer conform to the reasonable expectations of Americans, nor do these distinctions serve the public interest. A growing chorus of academics argues that these distinctions do not make sense,[34/] and courts have had increasing difficulty applying ECPA. The Fifth Circuit described efforts to interpret the Wiretap Act as a "search for lightning bolts of comprehension [that] traverses a fog of inclusions and exclusions which obscures both the parties' burdens and the ultimate goal."[35/] The Ninth Circuit described this as a "complex, often convoluted, area of the law."[36/] In 2002 the Ninth Circuit said that Internet surveillance was "a confusing and uncertain area of the law" that is so out-dated that it is "ill-suited to address modern forms of communication."[37/] A district court in Oregon recently opined that email is not covered by the Constitution, while the Ninth Circuit has

---

[33/] Matt Komorowski, *A History of Storage Cost*, *available at* http://www.mkomo.com/cost-per-gigabyte (concludes that "space per unit cost has doubled roughly every 14 months," and states that "[s]everal terabyte+ drives have recently broken the $0.10/gigabyte barriers."); *see also* Digital Prosperity *supra* Note 5, at 8 (The falling cost of storage is "why Web companies like Google, Yahoo, and Microsoft are providing consumers with large amounts of free Web-based storage for their email, photos, and other files. For example, Google provides around 2.7 gigabytes (2,700 megabytes) of free storage for users of their Gmail e-mail service. If Google were to provide this service today using the technology of 1975 (in 2006 prices), it would cost them over $50 million per user! But because memory is now so cheap, Google and other companies can afford to give vast amounts of it away for free, paying for it through unobtrusive advertisements.").

[34/] *See, e.g.*, Patricial L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev 1375, 1396-1397 (2004) (stating that "[s]tored communications have evolved in such a way that [ECPA's layer of statutory protection for stored communications], often referred to as the Stored Communications Act ("SCA"), are becoming increasingly outdated and difficult to apply."); 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, 1234 (2004) (stating that the "strange" 180-day distinction "may reflect the Fourth Amendment abandonment doctrine at work," but concluding that "[i]ncorporating those weak Fourth Amendment principles into statutory law makes little sense").

[35/] *Briggs v. Am. Air Filter Co.*, 630 F.2d 414, 415 (5th Cir. 1980) (Goldberg, J.). In a case involving the Wiretap Act and the Stored Communications Act, the same court said that the law is "famous (if not infamous) for its lack of clarity." *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994).

[36/] *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998).

[37/] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). The Ninth Circuit blamed this confusion on Congress's failure to update the law to take into account modern technologies. In particular, the court complained that: "the difficulty [in construing the surveillance statutes] is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication.… Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results." *Id.* While the Internet (but not the World Wide Web) did exist in 1986, it is entirely true that the Internet of 2010 bears very little resemblance to the Internet of 1986.

held that it is.[38/] Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion.[39/] The degree of uncertainty surrounding judicial application of ECPA requirements in any given situation makes it difficult for law enforcement and service providers alike to act with confidence. The absence of clear, intuitive rules necessarily complicates—and slows—business review of law enforcement requests. The absence of clear rules also makes businesses hesitant to embrace emerging Internet hosted services and complicates efforts to consolidate global data repositories.

As the Supreme Court has noted, clarity in the Fourth Amendment context benefits the public and law enforcement alike.[40/] Without clear rules, law enforcement personnel must either take the chance of stepping over the line-risking suppression of evidence or even personal sanctions - or shy away from the line to avoid overstepping.[41/] Neither law enforcement nor the public are well served when law enforcement cannot make appropriate use of an investigative tool because they do not know what is and is not allowed. A dramatic example of the negative consequences of the lack of clarity was cited by the Foreign Intelligence Surveillance Court of Review in *In Re Sealed Case*, where the court noted that the rules set forth in prior judicial decisions had been "very difficult… to administer."[42/] As the 9/11 Commission explained, in the days leading up to the 9/11 attacks, certain intelligence information was not shared with FBI agents who were familiar with al Qaeda because an intelligence analyst misunderstood those decisions and misapplied the Justice Department's rules implementing them.[43/] Lack of statutory

---

[38/] *Compare In re United States*, 2009 WL 3416240 (D. Or. June 23, 2009), *with Quon v. Arch Wireless Operating Co.*, 529 F.3d. 892, 895-899 (9th Cir. 2008), *cert. granted* 130 S. Ct. 1101 (2009).

[39/] *Warshak v. United States*, 490 F.3d 455, 467 (6th Cir.2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

[40/] *See, e.g., Arizona v. Roberson*, 486 U.S. 675, 681-682 (1988); *Oliver v. U.S.* , 466 U.S. 170, 181-182 (1984) ("This Court repeatedly has acknowledged the difficulties created for courts, police, and citizens by an ad hoc, case-by-case definition of Fourth Amendment standards to be applied in differing factual circumstances. The ad hoc approach not only makes it difficult for the policeman to discern the scope of his authority; it also creates a danger that constitutional rights will be arbitrarily and inequitably enforced." (citations omitted)).

[41/] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev 503, 527-528 (2007) ("The Fourth Amendment's suppression remedy … generates tremendous pressure on the courts to implement the Fourth Amendment using clear ex ante rules rather than vague ex post standards…. Clear rules announce ex ante what the police can and cannot do; so long as the police comply with the clear rules, the police will know that the evidence cannot be excluded.").

[42/] *In re Sealed Case*, 310 F.3d 717, 743-744 (FISA Ct. Rev. 2002).

[43/] *See id.* at 744; National Commission Terrorist Attacks Upon the United States, The 9/11 Commission Report at 78-80, 271, *available at* http://www.gpoaccess.gov/911/pdf/fullreport.pdf.

clarity also causes judicial uncertainty. When unclear statutory terms are interpreted differently in different federal jurisdictions, prosecutors are left with two choices: create different practices and procedures in each jurisdiction or adopt the most restrictive interpretation throughout the whole country. The first option can lead to confusion and arbitrary results, and the second can cause agents to forego the use of important investigative tools even where their use would be permissible.

As email has become a key means of personal and proprietary communications, and as users interact seamlessly with locally stored content and content stored on the Internet, ECPA's rules defy user expectation. Today, tens of millions of consumers enjoy free email and data storage services on the Internet.[44] These services are normally advertising-supported, and service providers use automated tools to scan the communications in order to deliver relevant advertising or other services.[45] Many service providers also examine content for security and anti-spam purposes.[46] All of these activities are undertaken in connection with providing the communication service, and users do not expect that these activities somehow render their private communications less private. Indeed, the average webmail user would be surprised to learn that the government believes this to be the case. Applying ECPA to normal business practices in a manner that deprives users of basic privacy protections threatens to undermine information technology innovations such as cloud computing, which, "by altering the basic economics of access to computing and storage … has the potential to reshape how U.S. and global businesses are organized and operate."[47]

---

[44] *See* Byron Acohido, *Microsoft takes notice as more people use free Google Docs*, USA Today, Sep. 22, 2009 (reporting that by July 2010 27% of companies plan to widely use Google Docs in the workplace).

[45] *See* Google, More on Gmail and privacy, *available at* http://mail.google.com/mail/help/about_privacy.html#scanning_email

[46] *See id*. ("Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do.")

[47] Jeffrey Rayport & Andrew Heyward, Andrew: *Envisioning the Cloud: the Next Computing Paradigm* (Mar. 20, 2009). According to the authors, cloud computing will lower capital requirements for technology start-ups, permit businesses to manage IT resources without tying up capital in IT capacity, while managing energy resources more efficiently; facilitate consumer access to an endless array of powerful applications at low cost; support innovation by reducing the human investment needed to build and maintain IT infrastructure; and foster cooperation and collaboration, without the coordination costs typically associated with bringing people and work together. *See* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf

As presently applied, ECPA does not comport with user expectations, does not meet law enforcement or judicial needs for clarity, creates non-trivial costs for businesses seeking to comply with law enforcement requests, and erects barriers to the adoption of innovative, productivity enhancing technology by American business. To address these deficiencies in a technology neutral manner, the consensus principles would bring all communications content, whether in transit or in storage (as commonly defined), notwithstanding the age of that content or the ordinary uses of that content by providers, under the basic probable cause standard set forth in the Fourth Amendment, accessible to law enforcement with a warrant.

Effect on Law Enforcement: This proposal would do no more than strictly necessary to reflect the reasonable expectations of privacy of communications technology users today, and to serve the public interest in facilitating innovation in the cloud. For example, the change:

- Would *not* extend to stored content the full range of protections that apply to real-time interception of communications content under the Wiretap Act, and would not require a "super warrant" for access to that data. Rather, this proposal does not modify the Wiretap Act,[48/] and under the proposal, a search warrant supported by probable cause would suffice to require a provider to disclose stored content;

- Would *not* further restrict the authority to access communications that are readily accessible to the general public, such as remarks posted on a blog or website available to the public;[49/]

- Would *not* modify the right of any authorized recipient of a communication, other than

---

[48/] In 2000, the Justice Department supported legislation that would have extended the procedural protections accorded to voice interceptions to the real-time interception of electronic communications under the Wiretap Act, a change that the Justice Department supported in 2000. *See* Testimony of Kevin V. DiGregory, Deputy Assistant Attorney General, United States Department of Justice, Before the Subcommittee on the Constitution of the House Committee on the Judiciary on H.R. 5018 and H.R. 4987 (Sep. 6, 2000) ("For example, the Administration's package proposes that wiretaps for electronic communications should be treated just the same as voice wiretaps, including approval by a high-level Justice Department official, limited to the list of predicate crimes under §2516, and with the availability of suppression under §2515."), *available at* http://judiciary.house.gov/Legacy/digr0906.htm.

[49/] 18 U.S.C. § 2511(2)(g)(1).

the service provider, to disclose data to the government without process. Thus, for example, anyone other than the service provider with authorized access to shared photos could voluntarily disclose those photos to anyone else, including a government agent;[50/]

- Would *not* change or eliminate any of the current exceptions permitting disclosures to the government by ECS and RCS providers, including those regarding inadvertently discovered evidence of a crime and emergency disclosures;

- *Would* establish uniform, clear, and easily understood rules about when and what kind of judicial review is needed by law enforcement to access electronic content; and

- *Would*, by clarifying the applicable rules, enable business to respond more quickly and with greater confidence to law enforcement requests and to avail themselves of hosted productivity technology.

Principle 2: Access to Mobile Location Data

Recommended Approach: Under the consensus principles, a governmental entity may require the provider of wire or electronic communications services to produce, prospectively or retrospectively, non-public information regarding the location of a mobile communications device only with a search warrant supported by probable cause.

Need for Change: Cell phones and mobile Internet devices generate location data to support both the underlying service and a growing range of location-based services of great convenience and value. A cell phone that is turned on—whether or not it is in use—is in near

[50/] One of the current exceptions—user consent—poses special issues, because, if broadly applied, consent would overwhelm all privacy protection. For government access, consent should not be inferred from, for example, Terms of Service that allow non-governmental entities to access content for various purposes. The recommendations are based on the presumption that the fact that a service provider has access to information in the cloud for purposes of providing the service, for offering value-added services or for delivering advertising does not diminish the user's expectation of privacy as against the government nor otherwise create any exception to the probable cause warrant requirement. This should be the case regardless of whether it is the provider or a third party contractor that is getting access for these business purposes. Rather, consent that would defeat the warrant requirement should have to be knowing, explicit, and specific both to the person who created the content and the content to be disclosed. If this is not clear, a further amendment may be appropriate.

constant communication with nearby cell towers,[51/] and, as a result, site tower information always reveals something about a user's location (*i.e.*, what tower or towers are nearby). In urban areas, where there are many cell towers, a mobile communications device may communicate its location to more than one tower. By triangulating information received by two or more cell towers, it is possible to establish a user's location within a matter of yards.[52/] This location data can be intercepted in real time and is often stored for research and development, resolution of billing disputes, and other business purposes;[53/] it can reveal a very full picture of a person's movements, leading to inferences about activities and associations. In a growing number of devices, this automatically generated location data is augmented by very precise GPS data.[54/]

The requirements governing access to location information are not clearly set out in ECPA. For years law enforcement treated cell site information as "signaling" or "addressing" information, obtained by simply certifying that the information—both retrospective and

---

[51/] *See* DOJ, *Electronic Surveillance Manual*, at 40 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ('MIN,' *i.e.*, telephone number) and electronic serial number ('ESN,' *i.e.*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode.")

[52/] *See id.* at 41. The Global Positioning System (GPS), cell towers, and Wi-Fi positioning service (WPS) are the three techniques to identify a mobile device geo-location.

[53/] *See* Declan McCullagh, *Feds Push for Tracking on Cell Phones*, Feb. 10, 2010, *available at* http://news.cnet.com/8301-13578_3-10451518-38.html ("Verizon Wireless keeps 'phone records including cell site location for 12 months,' [said] Drew Arena, Verizon's vice president and associate general counsel for law enforcement compliance.").

[54/] The FCC's Enhanced 9-1-1 service will by 2012 require wireless carriers to have the ability to report information about a caller's location to within 50 to 300 meters when the caller makes an emergency call, and within 100 meters for most such calls. 47 C.F.R. § 20.18(h)(1); *see* FCC Enhanced 9-1-1—Wireless Services, *available at* http://www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html. Wireless carriers often meet this requirement by installing GPS capabilities in their devices. For example, all Verizon devices sold after 2003 are GPS-capable. *See* http://aboutus.vzw.com/wirelessissues/enhanced911.html.

prospective—was "relevant to an ongoing investigation."[55/] In 1994 Congress amended the Pen Register statute to preclude the collection of information disclosing location "solely pursuant" to that statute.[56/] Notwithstanding this change, until 2005 judges routinely issued orders based on the "relevant to an ongoing investigation" certification so long as the request identified any additional authority for the request.[57/] Generally law enforcement cited the Stored Communications Act for this additional authority—even when the location information was sought on a prospective basis, on the theory that nothing in the Stored Communications Act "requires that the provider possess the records at the time the order is executed."[58/]

In 2005, a magistrate judge in the Southern District of Texas rejected this so-called "hybrid-theory," holding – as most cell phone users would assume - that prospective collection of cell site data amounted to "tracking." Citing the standard for installing a mobile tracking device under 18 U.S.C. § 3117, the magistrate judge determined that law enforcement could access prospective cell site data only with a warrant supported by probable cause.[59/] According

---

[55/] *See* DOJ, *Electronic Surveillance Manual*, at 45 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("In 1994, the Office of Enforcement Operations opined that investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture the numbers dialed or other information 'traditionally' collected using a pen/trap device. This analysis concluded that the 'signaling information' automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the 'contents' of a communication. Moreover, the analysis reasoned—prior to the 2001 amendments—that the pen/trap statute did not apply to the collection of such information because of the narrow definitions of 'pen register' and 'trap and trace device.' Therefore, the guidance concluded, since neither the constitution nor any statute regulated their use, such devices did not require any legal authorization to operate.")

[56/] Pub. L. 103-414, Title I, § 103 (1994) (codified at 47 U.S.C. § 1002(a)(2)). This preclusion is subject to an exception that applies to the extent the number itself provides the location, *i.e.*, for pay phones or wireline phones.

[57/] *See* DOJ, *Electronic Surveillance Manual* at 41, 43-44, *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("Because of the 1994 prohibition, law enforcement authorities have sought other means to compel providers to supply this information prospectively. Most commonly, investigators have used orders under section 2703(d) to obtain this information. Although section 2703(d) generally applies only to stored communications, nothing in that section requires that the provider possess the records at the time the order is executed. Moreover, use of such an order does not improperly evade the intent of the CALEA prohibition. Section 2703(d) court orders provide greater privacy protection and accountability than pen/trap orders by requiring (1) a greater factual showing by law enforcement and (2) an independent review of the facts by a court. Indeed, the very language of the CALEA prohibition—limiting its application 'to information acquired solely pursuant to the authority for pen registers and trap and trace devices'—indicates that Congress intended that the government be able to obtain this information using some other legal process. Public Law 103-414, sec. 103 (a) (emphasis supplied). Thus, 2703 (d) orders are an appropriate tool to compel a provider to collect cell phone location information prospectively." According to the DOJ Manual "[l]aw enforcement investigators may use … an order under section 2703(d) of title 18 in order to obtain historical records from cellular carriers.")

[58/] *Id.*

[59/] *In Re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority United States District Court*, Southern District of Texas, Houston Division, Magistrate No. H-05-557M (Oct. 14, 2005).

to Judge Smith, "While the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data." Magistrate judges around the country followed Judge Smith's lead on this, including a majority of the opinions published since 2005.[60/]

Although Judge Smith's opinion applied only to the *prospective* collection of cell-site information, he noted that an individual might have "an objectively reasonable privacy interest in caller location information,"[61] based on the Fourth Amendment as well as the Wireless Communication and Public Safety Act of 1999.[62/] He rejected the notion that there is no reasonable expectation of privacy in cell site location data, as well as the government's attempt to analogize cell site data to telephone numbers found unprotected in *Smith v. Maryland,* 442 U.S. 735 (1979): "Unlike dialed telephone numbers, cell site data is not "voluntarily conveyed" by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge … location information is a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer."[63/]

More recently, courts have rejected government requests for retrospective location data without a warrant, citing the language of the Stored Communications Act that "expressly sets movement/location information outside its scope by defining "electronic communications" to exclude "any communication from a tracking device" (as defined in 18 U.S.C. § 3117) and noting that the "electronic communications statutes, correctly interpreted, do not distinguish

---

[60/] *See* Declan McCullagh, *Feds Push for Tracking on Cell Phones*, Feb. 10, 2010, *available at* http://news.cnet.com/8301-13578_3-10451518-38.html ("Only a minority [of judges] has sided with the Justice Department [on rules regarding prospective cell phone tracking]."); Transcript of Town Hall Record, *Beyond Voice: Mapping the Mobile Marketplace*, at 177-178 (May 6, 2008) (Session 4, "Location-Based Services"), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/050608_sess4.pdf.

[61] *In Re Application for Pen Register*, supra note 58 at 16.

[62/] Pub. L. No. 106-81, § 5, 113 Stat. 1288 (Oct. 26, 1999) (codified at 47 U.S.C. § 222(f)).

[63/] *In Re Application for Pen Register*, supra note 58 at 15; http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

between historic and prospective [cell site location information]."[64/] Under these holdings, law enforcement can no longer assume that they will be able to acquire location data without a warrant based on probable cause.

Courts that require law enforcement to secure a warrant based on probable cause to access mobile location data recognize that users are likely to assume that tracking, however accomplished, is still tracking. To comport with reasonable expectations and serve the public interest, the current uncertainty should be resolved by applying the probable cause standard to disclosure of relatively precise location information.

There are already a number of innovative, socially beneficial "location aware" applications that employ technologies such as GPS, cell phone infrastructure, or wireless access points to locate electronic devices and provide "resources such as a 'you are here' marker on a city map, reviews for restaurants in the area, a nap alarm triggered by your specific stop on a commuter train, or notices about nearby bottlenecks in traffic."[65/] More applications such as these are emerging every day, and in short order "systems which create and store digital records of people's movements through public space will be woven inextricably into the fabric of everyday life."[66/] These applications will enhance quality of life, further important economic and social goals, and—with appropriate safeguards—serve law enforcement. Absent clear standards, privacy concerns could discourage consumer use, which could in turn make it less likely that location data will be available to law enforcement with proper authority.

64/ *In the Matter of the Application of the United States of America for an Order Directing the Provider of Electronic Communications Service to Disclose Records to the Government*, U.S. District Court for the Western District of Pennsylvania. Magistrate's No. 07-524M Magistrate Judge Lisa Pupo Lenihan , *aff'd* Sep. 2008, ("Government's requests for Court Orders mandating a cell phone service provider's covert disclosure of individual subscribers' (and possibly others') physical location information must be accompanied by a showing of probable cause."). The case has been appealed to the Third Circuit, which heard oral arguments on February 12, 2010. Case 08-4227.

65/ *See* Educause Learning Initiative, *7 Things You Should Know About … Location Aware Applications*, *available at* http://net.educause.edu/ir/library/pdf/ELI7047.pdf.

66/ Andrew J. Blumberg & Peter Eckersley, Electronic Frontier Foundation, *On Locational Privacy, and How to Avoid Losing it Forever*, at 1 (Aug. 2009), *available at* http://www.eff.org/files/eff-locational-privacy.pdf. The sensitivity of precise geographic location information was also discussed at a panel on mobile "location-based services" during the FTC's 2008 Town Hall on mobile marketing. *See* Transcript of Town Hall Record, *Beyond Voice: Mapping the Mobile Marketplace* (May 6, 2008) (Session 4, "Location-Based Services"), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/050608_sess4.pdf.

Effect on Law Enforcement: Information that reveals an individual's precise location can be highly sensitive, and collection of this information without proper safeguards implicates the exercise of a variety of rights protected by the Constitution, including important expression and association rights. To facilitate innovation, encourage the uptake of emerging location-aware technologies, and ensure that law enforcement access to location information generated by these products and services comports with the reasonable privacy expectations of Americans, ECPA should be amended to require a warrant based on probable cause to support access to location information, whether it is sought on a retrospective or prospective basis.[67/] This standard is consistent with Fourth Amendment safeguards against unreasonable search and seizure. In many cases, law enforcement must already meet the probable cause standard when requesting location data,[68/] and certain service providers are taking the position that location data is subject to higher standards under ECPA for content.[69/]

Principle 3: Access to Transactional Data

Recommended Approach: Under the consensus principles, a governmental entity could require the provider of wire or electronic communications services to produce, prospectively or in real time, transactional information (*i.e.*, dialed number information, IP address, Internet port information, email to/from information and similar communications traffic data)[70/] only with a judicial finding that the entity has offered specific and articulable facts demonstrating reasonable

---

67/ This would be subject, of course, to the exception for telephone numbers that themselves provide location information.

68/ Most courts have held that prospective information requires a showing of probable cause. See *supra* note_ 63. Law enforcement requests for retrospective location data are often combined with requests for prospective data. *See, e.g., In re Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, 534 F. Supp. 2d 585, 589 (W.D. Pa. 2008); *In re Application of U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448, 453 (S.D.N.Y. 2006).

69/ For example, the Loopt service "shows users where friends are located and what they are doing via detailed, interactive maps on their mobile phones.… Users can also share location updates, geo-tagged photos and comments with friends in their mobile address book or on online social networks, communities and blogs." The provider clearly understands the privacy implications of this technology, and reassures users that "Loopt was designed with user privacy at its core and offers a variety of effective and intuitive privacy controls." About Loopt, *available at* http://www.loopt.com/about.

70/ DOJ, *Electronic Surveillance Manual*, at 39 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("Pen register and trap and trace devices may obtain any noncontent information—all 'dialing, routing, addressing, and signaling information'—utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the 'To' and 'From' information contained in an e-mail header.")

grounds to believe the information sought is relevant and material to an ongoing criminal investigation.

Need for Change: Transactional data—records of who is calling whom, when and for how long, and records of all the "to" and "from" information associated with one's email, including date, time, message length (including subject line length)—can be highly revealing. Transactional records for e-mail and cell phone usage may contain far more information about an individual's communications than "pen register" data in the wireline environment of the 1980s.[71] As technology has evolved, transactional data has become ever more detailed and revealing, but remains available to law enforcement without effective judicial supervision. In fact, under ECPA, a court *must* issue an order for a pen register[72] or trap and trace device[73] whenever a prosecutor files a document stating that the information sought is relevant to an ongoing investigation.[74] Thus, read literally, a judge cannot even assess whether the information is in fact relevant; the only question is whether the government says that it is. As communications technology evolves and produces increasingly detailed and rich transactional

---

[71] For example, the transactional record of an outgoing phone call to someone in a large office likely only contains the general office phone number and does not specify which person in the office has been contacted. However, the transactional record of an email to that person contains the recipient's unique email address. *See* Center for Democracy & Technology's Analysis of S.2092 (Apr. 4, 2000), *available at* http://old.cdt.org/security/000404amending.shtml.

It is not yet clear whether information such as URL's that include search terms or specific website addresses are "content" information that must be excluded from transactional records. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev 2105, 2105 (2009) ("Courts and Internet law scholars have yet to offer a means of determining the content/envelope status of unique aspects of Internet communications-from email subject lines to website URLs."). If transactional records for e-mail or Internet-enabled cell phones include this information, then they would be far more revealing than traditional wireline telephone records. *E.g.*, *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) ("Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity.").

[72] A "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication…." 18 U.S.C. § 3127(3).

[73] A "trap and trace device" is defined as a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, [or] signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however that such information shall not include the contents of any communication. 18 U.S.C. § 3127(4).

[74] 18 U.S.C. § 3123(a).

information, it is appropriate to afford judges a meaningful role in assessing whether the government's claim of relevance is substantiated.

Effect on Law Enforcement: The Justice Department has in the past acknowledged that the approach taken by the recommended principle is appropriate.[75/] Nonetheless, the consensus principles call for a modest change only: The standard proposed is significantly less than probable cause: "specific and articulable facts showing that there are reasonable grounds to believe that the information … is relevant and material." Drawn from the *Terry* decision of the U.S. Supreme Court,[76/] the language is identical to the formulation in the Stored Communications Act, which currently provides:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[77/]

The marginal burden on law enforcement from this change should be minimal because law enforcement rarely asks for a pen register order without already possessing information sufficient to satisfy a "specific and articulable facts" standard.[78/] The change will enhance business

---

[75/] *See* DOJ's View on H.R. 5018 (Electronic Communications Privacy Act of 2000), Testimony of Kevin Digregory, Deputy Associate Attorney General, *available at* http://commdocs.house.gov/committees/judiciary/hju67343.000/hju67343_0.htm ("H.R. 5018, like the Administration's bill, would introduce the requirement of judicial review of the factual basis for such orders. Specifically, H.R. 5018 would require such applications to contain 'specific and articulable facts' that would justify the collection of the data. While the Justice Department can comply with the added administrative burdens imposed by increasing this standard, we have concerns about the amendments. Specifically, the technology-specific manner in which the bill would implement this change, the lack of an emergency exception, and the unrealistic geographic limitations that restrict such orders in the present law all raise serious concerns that should be addressed.").

[76/] *Terry v. Ohio*, 392 U.S. 1, 21 (1968).

[77/] 18 U.S.C. § 2703(d).

[78/] Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 639 & 673 n. 154 (2003) ("[A] higher 'specific and articulable facts' threshold would not add substantial burden for law enforcement…. [I]n my government experience I never knew or even heard of any law enforcement agent or lawyer obtaining a pen register order when the agent did not also have specific and articulable facts, which would satisfy the higher threshold. My experience is narrow, but it suggests that the practical burden of obtaining the order combined with the certification to a federal judge and potential for criminal liability effectively regulates government officers and deters them from obtaining pen register orders in bad faith. On the other hand, there may be rogue officers out there, if not now then in the future, and a higher threshold combined with judicial review could potentially provide an extra barrier to abuse.").

responsiveness by clarifying the obligations of both law enforcement and business, and preserves the distinction between content and transactional data, and maintains the reduced burden needed to acquire the latter.

Principle 4: Access to Subscriber Identifying Data and Stored Transactional Information

Recommended Approach: Under the consensus principles, a governmental entity may use a subpoena to require the provider of wire or electronic communications services to produce information related to a specified account or individual. Judicial approval would be necessary only where such requests do not relate to a specified account or individual.

Need for Change: Under ECPA, law enforcement may use an administrative, grand jury or trial subpoena to acquire certain information pertaining to a "subscriber to or [a] customer" of an electronic communications service or remote computing service.[79/] The information that may be acquired under this provision includes name, address, call or session records, length of service and type of service utilized, and method of payment.[80/] Using the administrative subpoena authority, law enforcement makes an independent determination that certain records are needed and then issues and serves the subpoena without input from a grand jury or even an assistant U.S. Attorney. Such administrative subpoenas are subject to judicial review only if the recipient of the subpoena challenges it. With administrative, grand jury or trial subpoenas, the government has no obligation to notify the subscriber or customer to whom the records relate.[81/] A carrier or ISP will rarely have the incentive to challenge a subpoena, so this information is routinely disclosed without any judicial review whatsoever.

The absence of judicial review or any meaningful opportunity to challenge a request for subscriber identifying records and stored customer records suggests that the scope of the subpoenas in these cases should be appropriately tailored. Indeed, the language of the statute itself suggests that such subpoenas may be issued for information pertaining to "a subscriber" or "a customer" identified with some particularity, for example, by a phone number or an IP

79/ 18 U.S.C. § 2703(c)(2).

80/ *Id.*

81/ 18 U.S.C. § 2703(c)(3).

address at a specific time. This principle would make it clear that a subpoena cannot be used to compel production of, for example, information identifying "*all* subscribers" whose device registered on a specified cell tower on a specified date, or information identifying "*all* subscribers" who accessed a particular web site during a specified period of time. Nothing in the legislative history of ECPA suggests that the provision should be read to authorize such broad use of subpoenas. Rather, the absence of judicial review argues for a narrow interpretation to avoid misuse of the subpoena for "fishing expeditions."[82/]

Effect on Law Enforcement: The principle is intended to clarify that the government may use a subpoena to obtain the subscriber information specified in the statute if the investigator can identify the subscriber with particularity (*e.g.* phone number, IP address used at a specific time). Otherwise, the investigator would obtain the information after securing a §2703(d) order based on specific and articulable facts demonstrating reasonable grounds to believe that the information is relevant to an ongoing criminal investigation, or a search warrant. The consensus principles would leave the current standard found in ECPA untouched when the records sought by law enforcement pertain to a specific subscriber or customer. Only if the government sought records about groups of subscribers or customers, would judicial review be required.

Conclusion

The United States leads the world in bringing innovative, ground-breaking communications technology to market, and enjoys the many social and economic benefits that technology produces. The United States also enjoys the many benefits flowing from Constitutional safeguards designed to preserve individual liberties, including the right to be free from unreasonable search and seizure. The U.S. has consistently balanced those values with the

---

82/ Without a narrow interpretation, law enforcement can subpoena a list of all visitors to a news website on a particular day, and order that the recipient of the subpoena not disclose the subpoena's existence. The Department of Justice recently attempted this before withdrawing its subpoena after the website owners objected publicly. *See* Declan McCullagh, *Justice Dept. Asked for News Site's Visitor Lists*, Taking Liberties Blog (Nov. 10, 2009), *available at* http://www.cbsnews.com/blogs/2009/11/09/taking_liberties/entry5595506.shtml; Copy of Subpoena, *available at* http://www.eff.org/files/subpoena.pdf. *See also* Nymity Interview, *Where Did Due Process Go? Government Access to Personal Information in the Cloud* (Interview with Scott Shipman, eBay) (Feb 2010), http://www.nymity.com/Free_Privacy_Resources/Privacy_Interviews/2010/Scott_Shipman.aspx ("[W]e're starting to see a new wave of requests. These new requests are a broad request for a large group of unnamed customers. For example, we see requests from authorities that state, 'please provide all information on all sellers who have sold in the following jurisdiction (zip code) within the last year.' Requests like those arguably flip the notion of due process upside down.").

needs of law enforcement in the communications environment, and both U.S. consumers and the U.S. economy have benefitted from the trust and confidence that this balance inspires in our electronic communications and information technology services providers, including among businesses and individuals located outside our borders. Changes in technology since 1986 have made it difficult to apply ECPA in a manner that comports with the reasonable expectations of individuals, potentially eroding user willingness to entrust private information to third party service providers in the United States. The principles recommended by the working group would, if implemented, align ECPA with current and emerging technology without unduly constraining or imposing significant burdens on law enforcement.