Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director
ACLU Washington Legislative Office

Christopher Calabrese
Legislative Counsel
ACLU Washington Legislative Office

Nicole A. Ozer, Esq.
Technology and Civil Liberties Policy Director
ACLU of Northern California

before the
Senate Judiciary Committee

September 22, 2010

Hearing on

The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age

Chairman Leahy, Ranking Member Sessions, and Members of the Committee:

The American Civil Liberties Union (ACLU) has over half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government. Throughout our history, we have been one of the nation's foremost protectors of individual privacy. We write today to urge the committee to take the first steps toward modernizing the Electronic Communications Privacy Act (ECPA).

The Founding Fathers recognized that citizens in a democracy need privacy for their "persons, houses, papers, and effects." That remains as true as ever. But our privacy laws have not kept up as technology has changed the way we hold information. Thomas Jefferson knew the papers and effects he stored in his office at Monticello would remain private. Today's citizens deserve no less protection just because their "papers and effects" might be stored electronically.

The main statutory protection for the privacy of communications, ECPA, was written in 1986 before the Web was even invented. Technology has not only advanced tremendously since 1986, it has also become an essential part of our lives. It impacts how we learn, share, shop and connect. We need an updated ECPA to match our modern online world.

Americans Have Embraced Technology

Technology has changed immensely since ECPA was written in 1986—and Americans have adopted these changes into their lives:

- Over 50% of American adults use the Internet on a typical day.[1]
- 62% of online adults watch videos on video-sharing sites,[2] including 89% of those aged 18–29.[3]
- 69% of online adults use "cloud computing"[4] services to create, send and receive, or store documents and communications online.[5]

---

[1] Common daily activities include sending or receiving email (40+% of all American adults do so on a typical day), using a search engine (35+%), reading news (25+%), using a social networking site (10+%), banking online (15+%), and watching a video (10+%). Pew Internet & American Life Project, *Daily Internet Activities, 2000–2009*, http://www.pewinternet.org/Trend-Data/Daily-Internet-Activities-20002009.aspx.

[2] A "video-sharing site" or "video hosting site" is a website that allow users to upload videos for other users to view (and, often, comment on or recommend to others). Wikipedia, *Video Hosting Service*, http://en.wikipedia.org/wiki/Video_sharing (as of May 1, 2010, 04:21 GMT). YouTube is the most common video-sharing site today.

[3] Pew Internet & American Life Project, *Your Other Tube: Audience for Video-Sharing Sites Soars*, July 29, 2009, http://pewresearch.org/pubs/1294/online-video-sharing-sites-use

[4] The term "cloud computing" has many definitions, but generally refers to services that offer applications or data storage accessible via the web. Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services*, Sep. 2008 [hereinafter Pew Cloud Report], http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx.

[5] Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services*, Sep. 2008 [hereinafter Pew Cloud Report], http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-

- Over 70% of online teens and young adults[6] and 35% of online adults have a profile on a social networking site.[7]
- 83% of Americans own a cell phone and 35% of cell phone owners have accessed the Internet via their phone.[8]
- One in four U.S. adults have used a location-based service[9], and two-thirds of iPhone users access a location-based service at least once a week.[10]

Companies continue to innovate and create new ways for Americans to merge technology with daily activities. Google has spent the last five years building a new online book service and sales of digital books and devices have been climbing.[11] Americans increasingly turn to online video sites to learn about everything from current news to politics to health.[12] As the recently announced Facebook location service "Places" heralds, location-based services are a burgeoning market.[13] There are thousands of location-aware applications available for the 49 million smartphone users in the United States.[14]

These services provide many benefits, but they also have the ability to collect and retain detailed information about individuals: their interests, concerns, movements, and associations. This information can be linked together, allowing a user's Internet searches, emails, cloud computing

---

Services.aspx . 56% of Internet users use webmail services, 34% store photos online, and 29% use online applications such as Google Docs or Adobe Photoshop to create or edit documents.

[6] Pew Internet & American Life Project, *Social Media & Young Adults*, Feb. 3, 2010, http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

[7] "Social networking sites" allow users to construct a "semi-public" profile, connect with other users of the service, and navigate these connections to view and interact with the profiles of other users. danah m. boyd & Nicole B. Ellison, *Social Networking Sites: Definition, History, and Scholarship,* 13 J. of Comp.-Mediated Comm. 1 (2007); Pew Internet & American Life Project, *Adults & Social Network Sites*, Jan. 14, 2009, http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx.

[8] Pew Internet & American Life Project, *Internet, Broadband, and Cell Phone Statistics*, Jan. 5, 2010, http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.

[9] "Location-based services" is an information service utilizing the user's physical location (which may be automatically generated or manually defined by the user) to provide services. Wikipedia, *Location-Based Service*, http://en.wikipedia.org/wiki/Location-based_service (as of May 1, 2010, 04:35 GMT).

[10] Mobile Marketing Ass'n, U.S. Consumers Significantly More Likely to Respond to Location-Based Mobile Ads than Other Mobile Ad Types, Apr. 21, 2010, http://mmaglobal.com/news/us-consumers-significantly-more-likely-respond-location-based-mobile-ads-other-mobile-ad-types.

[11] *See generally* ACLU of Northern California, *Digital Books: A New Chapter for Reader Privacy*, Mar. 2010, *available at* http://www.dotrights.org/digital-books-new-chapter-reader-privacy.

[12] "More Americans are watching online video each and every month than watch the Super Bowl once a year." Greg Jarboe, *125.5Million Americans Watched 10.3 Billion YouTube Videos in September*, SEARCHENGINEWATCH.COM, Oct. 31, 2009, http://blog.searchenginewatch.com/091031-110343.

[13] Recent location-based service Foursquare built a base of 500,000 users in its first year of operation. Ben Parr, *The Rise of Foursquare in Numbers [STATS]*, MASHABLE, Mar. 12, 2010, http://mashable.com/2010/03/12/foursquare-stats/.

[14] Mobile Subscriber Market Share, July 8, 2010, http://www.comscore.com/Press_Events/Press_Releases/2010/7/comScore_Reports_May_2010_U.S._Mobile_Subscriber_Market_Share; Skyhook Wireless, Location Aware App Report, Feb. 2010 http://www.locationrevolution.com/stats/skyhookfebreport.pdf.

documents, photos, social networking activities, and book and video consumption to be collected into a single profile.[15]

Americans Still Expect Privacy

This rapid adoption of new technology has not eliminated Americans' expectations of privacy. To the contrary, Americans still expect and desire that their online activities will remain private, and express a desire for laws that will protect that privacy.

- 69% of Internet users want the legal right to know everything that a Web site knows about them.[16]
- 92% want the right to require websites to delete information about them.[17]
- A large percentage of users of cloud computing are "very concerned" about how their personal information may be used and disclosed to law enforcement and third parties.[18]

When user privacy is not protected, users are slower to adopt new technology. A recent poll revealed that 50% of Americans polled have little or no interest in using cloud computing and that 81% of these respondents are reluctant, at least in part, because they are concerned about the security of their information in the cloud.[19]

Americans want and need legal protections for privacy that reflect the technology they use every day. The time has come to modernize ECPA to reflect our 21st century digital world.

ECPA Rules Are Confusing and Outdated

In the face of rapid technological change and Americans' continuing expectation of privacy, ECPA has fallen behind. Distinctions in ECPA have become increasingly confusing and arbitrary, based on an understanding of technology that is a generation behind that which we use today.[20] Many new technologies, particularly those dealing with location information, are not addressed by ECPA. These failures not only leave holes in the privacy protections in place for individuals, but pose a threat to continuing innovation and business development. We need to update ECPA to encompass all of the ways that Americans use technology today.

---

[15] *See* ACLU of Northern California, *Digital Books*, *supra* note 11 ("[I]f a reader has logged in to other Google services such as Gmail at the time he searches for a book, Google can link reading data to the reader's unique Google Account [and] retains the right to combine all this information with information gleaned from its DoubleClick ad service, which tracks users across the Internet.") More information is available at the ACLU's Demand Your dotRights campaign website. Demand Your dotRights, http://dotRights.org.

[16] Joseph Turow, et al., *Americans Reject Tailored Advertising* 4 (2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[17] *Id.*

[18] Cloud computing users are "very concerned" about law enforcement access to data (49%); services retaining files after users delete them (63%); services using personal data for targeted advertisements (68%) or marketing (80%); services selling files or data to third parties (90%). See Pew Cloud Report, *supra* note 5, at 11.

[19] Harris Interactive, *Cloud Computing: Are Americans Ready?*, Apr. 21, 2010, http://news.harrisinteractive.com/profiles/investor/ResLibraryView.asp?BzID=1963&ResLibraryID=37539&Category=1777.

[20] *See Steve Jackson Games v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994) (The Wiretap Act, as amended by ECPA, is "famous (if not infamous) for its lack of clarity.").

E-mail exemplifies the gap between the language of ECPA and today's technology. In 1986, e-mail was typically downloaded to a recipient's computer upon receipt and immediately deleted from the e-mail provider's storage. ECPA was written with this behavior in mind: it requires a search warrant to retrieve a message from an e-mail provider's storage only if the message is less than 180 days old, and provides for lower standards if the email is left on the server for more than 180 days.[21] Today, however, e-mail is often both stored on and accessed from remote servers belonging to the e-mail provider, and many people "archive" their e-mail on their provider's server rather than deleting old messages. Basing legal protection on how long an e-mail has been stored is incongruous with current e-mail use. Instead, ECPA should provide full protection for all online documents and communications and dispose of these artificial and outdated distinctions.

Similarly, the state of technology in 1986 resulted in more legal protection in ECPA for the content of communication—the body of an e-mail or the contents of a letter or phone conversation—than for the transactional information. Historically, transactional information was easy to distinguish from content: the number dialed on a telephone as opposed to the voice call itself, or writing on the outside of an envelope as opposed to the message within. The digital world, however, blurs the line between content and transactional data. Internet search terms, browser history, e-mail subject lines and location information do not fit neatly into either category and can reveal sensitive data like political and religious affiliations. Most people consider such information to be private. The law should match these expectations and require a warrant for disclosure.

In addition to the difficulty in anticipating modern uses of technologies existing in that era, lawmakers in 1986 could not predict technological innovations. Mobile phones provide a glaring example, along with the location information gleaned from them. Modern cell phones have become, in essence, portable tracking devices. Technologies including GPS[22] and cell tower triangulation[23] allow mobile phone providers to determine our physical locations in real time and retain records of this location information indefinitely. The legal standard for access to these records is currently being litigated, and Congress has never weighed in on what the appropriate standard should be.[24] In the meantime, law enforcement agents are already aggressively seeking massive amounts of information about consumer location. In 2009, a company employee provided a rare glimpse into the scope of government demands for location data when he

---

[21] Even this limited protection is in doubt. The Department of Justice has argued that, once email is opened, it is no longer in "electronic storage" and thus no longer subject to a warrant requirement under ECPA even if it is less than 180 days old. *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), D. Colo., No. 09-80.*

[22] GPS, or Global Positioning System, is a satellite-based navigation system that allows a GPS receiver to determine its own location. *Global Positioning System*, http://gps.gov.

[23] Cell tower triangulation allows the location of a mobile device to be determined by "triangulation" based on its calculated distance from two or more cell towers within the phone's range. *See* Chris Silver Smith, *Cell Phone Triangulation Accuracy Is All Over the Map*, SearchEngineLand.com, Sep. 22, 2008, http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790.

[24] *See, e.g., In re Application of the United States for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government*, No. 08-4227 (3d. Cir. Sept. 7, 2010) (finding a judge may require law enforcement to show probable cause before obtaining historical cell site location information).

admitted that Sprint received a staggering eight million requests for mobile phone location information from law enforcement in just over a year.[25]

Unfortunately, this data is sometimes sought under questionable circumstances that highlight the potential for abuse. In 2008, the FBI sought and received (without a warrant) location-tracking information not just for a robbery suspect, but for 180 other innocent people;[26] in 2010, Michigan police officers sought information about every cell phones near the site of a planned labor protest;[27] and an Alabama sheriff demanded that a telecommunications company track his daughter's location without a warrant when she didn't come home from a date, claiming that she had been kidnapped.[28] These examples are likely just the tip of the iceberg.

Outdated digital privacy law is not only a threat to individual privacy; it also affects businesses and hinders innovation. User perception of inadequate privacy is one threat that companies face. For example, Microsoft recently announced that its future lies in online cloud computing services, but its own poll found that more than 90 percent of the general population is "concerned about the security, access, and privacy of personal data" stored online,[29] leading the company to explicitly ask Congress for better online privacy protection to promote cloud computing.[30]

Companies are also affected when they receive demands to turn over the personal information of users. Time Warner Cable employs 4 people dedicated solely to responding to law enforcement requests to look up Internet Protocol (IP) addresses.[31] In April 2010, Google released data that it received over 3,500 demands from law enforcement involving criminal investigations in the last six months of 2009.[32]

If Google is receiving thousands of demands digging into the intimate details of individual lives that are captured in emails, search histories, reading and viewing logs, and the like, how many more are going out to Yahoo, Microsoft, Facebook and the thousands of other online services that Americans use every day? And how can companies hope to respond to these requests

---

[25] Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year*, WIRED, Dec. 1, 2009.
[26] Brief of Amici Curiae in Support of Motion to Suppress, *United States v. Soto*, Case No. 09-cr-200 (D. Conn. June 18, 2010), *available at* http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf. While the details remain unclear because the government surveillance demands are under seal, it appears that the government engaged in dragnet surveillance, seeking and obtaining location information for a large number of innocent people to identify who was involved in the crime.
[27] *See* Michael Iskoff, *The Snitch in Your Pocket*, NEWSWEEK, Feb. 19, 2010.
[28] Transcript of "Where I'm Calling From," On the Media, May 8, 2009, *available at* http://www.onthemedia.org/transcripts/2009/05/08/05.
[29] Microsoft News Center, *Cloud Computing Flash Poll—Fact Sheet,* http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc. More information is available at http://www.microsoft.com/presspass/presskits/cloudpolicy/materials.aspx.
[30] Microsoft News Center, *Press Release: Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud*, Jan. 20, 2010, *available at* http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx.
[31] Nate Anderson, *Time Warner Tries to Put Breaks on Massive Piracy Case*, ARS TECHNICA, May 16, 2010, http://arstechnica.com/tech-policy/news/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case.ars.
[32] Government Requests Tool, http://www.google.com/governmentrequests. Note this does not include National Security letters or demands received outside of criminal investigations. It also does not count the actual number of users whose records disclosed pursuant to each demand. All of this means this number likely only reflects a fraction of the number of users whose records were demanded.

without improperly over- or under-disclosing information when faced with outdated, confusing laws with questionable applicability to their products or services?

Key Principles for Updating ECPA

Because these inadequate legal standards create difficulties for Internet users and businesses alike, a coalition of privacy advocates and businesses—from the American Civil Liberties Union to Google and AT&T—has formed to urge Congress to update electronic privacy law to provide clear rules and better protection for electronic data. The coalition believes that just as the law recognized that storing information in digital form on a computer hard drive should have the same probable cause warrant protection as information stored in paper form in a filing cabinet, the time has come to ensure that these same privacy protections apply to digital information stored in the cloud.

The ACLU believes the efforts being urged by the coalition to update ECPA are critical first steps but believes a full review of ECPA should involved all of the following issues:

1. Robustly Protect All Personal Electronic Information.
2. Safeguard Location Information.
3. Institute Appropriate Oversight and Reporting Requirements.
4. Require a Suppression Remedy.
5. Craft Reasonable Exceptions.

Robustly Protect All Personal Electronic Information.

In the modern world, just as in Jefferson's time, our personal, private information—whether paper documents and correspondence or records of what we search and read online—reveals a tremendous amount about us. Our right to privacy and our rights to free expression and free association require that this information be protected from disclosure to the government without notice and without a warrant based on probable cause. Changing technology must not erode these protections. Our e-mail, online spreadsheets and photos, and other digital documents need strong legal protections regardless of how, where, or how long they are stored.

But American's privacy interest is not limited to the content of communications. Congress has long-recognized the privacy interests in the transactional records of users of expressive material. The Video Privacy Protection Act prohibits disclosure of video viewing records without a warrant or court order, requires notice prior to any disclosure of personally identifiable information to a law enforcement agency, and requires the destruction of personally identifiable information one year after it becomes unnecessary.[33] The Cable Communications Policy Act similarly prohibits disclosure of cable records absent a court order.[34] Similarly, to safeguard autonomy, privacy, and intellectual freedom, our laws extend protection to library and book

[33] 18 U.S.C. § 2710(b)(2)(B), (b)(3),(e) (2009).
[34] 47 U.S.C. § 551(c) (2008).

records.[35] We need the same protection for digital records that implicate our First Amendment freedoms by recording our expressive actions and choices.

Current loopholes in our privacy laws need to be closed to protect electronic information without regard to its age, whether it is "content" or "transactional" in nature, or whether companies or individuals can use this information for other purposes. ECPA must be modernized to provide robust protection for all personal electronic information and require a probable cause warrant and notice prior to disclosure.

Safeguard Location Information.

The vast majority of Americans own cell phones. The location information transmitted by these phones every minute of every day reveals not only where we go but often what we are doing and who we are talking to. Americans take cell phones everywhere: to gun rallies, to mental health clinics, to church, and everywhere else we go. Ubiquitous tracking is a realistic possiblity in the United States. We must protect this sensitive information from inappropriate government access. Location information, whether current or historical, is clearly personal information. The law should require government officials to obtain a warrant based on probable cause before allowing access.

Institute Appropriate Oversight and Reporting Requirements.

Electronic recordkeeping enables easy collection and aggregation of records, and the insufficient and outdated standards applied by ECPA provide little barrier should the government wish to engage in a "shopping spree" through the treasure trove of personal information held by private companies. In addition to updating the standards for access to electronic information, ECPA should ensure adequate oversight by Congress and adequate transparency to the public by extending existing reporting requirements for wiretap orders to all types of law enforcement surveillance requests.

The House Judiciary Committee recognized this need when it approved HR 5018 (106th Congress) by a vote of 20-1.[36] The proposed bill would have required reporting on all orders, warrants, or subpoenas issued by government entities seeking electronic communications records or content information. Current efforts to modernize ECPA should include this requirement as well.

---

[35] 48 states protect library reading records by statute, *see, e.g.*, N.Y. C.P.L.R. § 4509; Cal. Gov. Code §§ 6267, 6254(j), and federal and state courts have also often frowned upon attempts by the government or civil litigants to gain access to such records, *see, e.g.*, *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 573 (W.D. Wis. 2007) (quashing a government subpoena seeking the identities of 120 book buyers because "it is an unsettling and un-American scenario to envision federal agents nosing through the reading lists of law-abiding citizens while hunting for evidence against somebody else."); *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (First Amendment requires government to "demonstrate a compelling interest in the information sought . . . [and] a sufficient connection between the information sought and the grand jury investigation" prior to obtaining book records); *Tattered Cover v. City of Thornton*, 44 P.3d 1044, 1059 (Colo., 2002) (government access to book records only passes muster under Colorado Constitution if "warrant plus" standard is met by the government—i.e, prior notice, adversarial hearing, and showing of a compelling need).

[36] H.R. Rep. No. 106-932 to accompany H.R. 5018 (2000) at 23.

Require a Suppression Remedy.

Both the Fourth Amendment and the Wiretap Act provide for an exclusionary remedy: if a law enforcement official obtains information in violation of a defendant's constitutional privacy rights or the Act, that information usually cannot be used in a court of law.[37] The same rule, however, does not apply to electronic information obtained in violation of ECPA. Without an exclusionary rule, there is a lack of deterrence for government overreaching. Unlawfully obtained electronic information should be barred from use in court proceedings. A suppression remedy provision passed the House Judiciary Committee in 2000 as part of HR 5018 and should be included in any current Congressional language to modernize ECPA.[38]

Craft Reasonable Exceptions.

Overbroad exceptions and the abuse of "voluntary disclosure" procedures are also depriving Americans of their rightful privacy protection. ECPA needs to be revised to close these loopholes and ensure that private information is only released outside of the standard process when truly necessary.

Under previous law, a company could only turn records over if it had a "reasonable belief" that there was an emergency involving "imminent harm" of death or injury to any person. However, in 2001 that standard was lowered so that the company's belief only needed to be held in "good faith" and that the harm no longer needed to be imminent. This lowered standard reduced a company's obligation to ensure that its decision to release private information about a user was balanced by the exigency of the situation.

In addition, exceptions to prohibitions on "voluntary" disclosure need to be revised to prevent coercive abuse by law enforcement. For example the Inspector General for the Department of Justice has reported that the FBI circumvented its National Security Letter (NSL) authority by using "exigent letters" to obtain information with the promise that the agent had already requested a grand jury subpoena or an NSL.[39] To prevent such abuse, all requests for "emergency" voluntary disclosures under ECPA should clearly state that compliance with the request is voluntary and ECPA should require thorough documentation and reporting of all such requests.

Exceptions to the procedural requirements for government access to electronic records should be just that: exceptional. ECPA reform should restore the original emergency exception for ECPA and require documentation and reporting to ensure that these exceptions are used properly and not abused.

Conclusion

[37] 18 U.S.C. 2515.
[38] Electronic Communications Privacy Act of 2000, H.R. 5018, 106th Cong. § 2 (2000).
[39] Dep't. of Justice, Office of Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters (March 2007), at 86–97, *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf.

We applaud the Committee for holding this hearing and for beginning to undertake the task of reforming ECPA. Changes in the way we communicate with each other in today's world are wondrous viewed through 1980s spectacles. That wonderment should not be tempered by the realization that our personal privacy is slipping away. Comprehensive reform of ECPA is a needed legislative initiative that will help preserve the real innovative value of the technology boom and set us on a path for even greater innovation to come.