WRITTEN STATEMENT OF
THE AMERICAN CIVIL LIBERTIES UNION

For a Hearing on

"ECPA Part 1: Lawful Access to Stored Content"

Submitted to the House Judiciary Committee
Subcommittee on Crime, Terrorism, Homeland Security and Investigations

March 19, 2013

ACLU Washington Legislative Office
Laura W. Murphy, Director
Christopher Calabrese, Legislative Counsel

The American Civil Liberties Union (ACLU) submits this statement to the House Judiciary Committee, on the occasion of its hearing addressing "ECPA Part 1: Lawful Access to Stored Content."[1] We offer this statement to highlight the changes in technology that have eroded American's traditional expectation of privacy and to urge the committee to take steps toward modernizing the Electronic Communications Privacy Act (ECPA) to address those changes.

The Importance of Privacy in the Digital Age

The Founding Fathers recognized that citizens in a democracy are entitled to privacy, writing in the Fourth Amendment that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause." 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 personal rooms at Monticello would remain private. Today's citizens deserve no less protection just because their "papers and effects" might be stored electronically.

The warrant and probable cause requirements are essential components of the Fourth Amendment. The function of the warrant clause is to safeguard the rights of the innocent by preventing the state from conducting searches solely at its discretion:

> Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done not to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted.[2]

This principle has long applied to communications as well. A probable cause warrant has been required for access to postal mail since at least the 1870s and for access to landline telephone calls since the 1960s.[3]

The warrant and probable cause requirements are especially important today given the extraordinary intrusiveness of modern-day electronic surveillance. As technology has advanced and we have entered the digital age, more and more of our personal information has been gathered, compiled, and stored in easily accessible forms. Private correspondence once took the form only of letters sent through the postal service. They were typically stored within the home, and were often irretrievably discarded after a few days. By contrast an individual's emails are

[1] The ACLU is a nationwide, non-partisan organization of more than a half-million members, countless additional activists and supporters, and 53 affiliates nationwide dedicated to enforcing the fundamental rights of the Constitution and laws of the United States. The ACLU's Washington Legislative Office (WLO) conducts legislative and administrative advocacy to advance the organization's goal of protecting the privacy rights of every American.

[2] *McDonald v. United States*, 335 U.S. 451, 455 (1948).

[3] *United States v. Warshak*, 631 F.3d 266.

typically stored by a third party on a centralized, remote server, can be searched easily for key terms or topics, and may never be deleted permanently.

Similarly, tracking an individual's movements for days or searching for the presence of one person over a large area would have once required a great deal of effort and enormous resources. But the rise of cell phone and GPS technology has made such operations as simple as a quick request to a service provider. As Justice Alito wrote in *United States v. Jones*,

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken… [technological advancements], however, make long-term monitoring relatively easy and cheap.[4]

The danger posed by unwarranted government intrusions into Americans' private lives has not changed, but the ease with which those intrusions can be undertaken has. Creating legal protections to safeguard the fundamental American value of privacy, as laid out by our Founders in the Fourth Amendment, has become ever more important. In order to protect that value, Congress must update the law surrounding the privacy of our electronic communications by modernizing ECPA.

Law Enforcement Access to the Content of Communication

When the original Electronic Communications Privacy Act was passed in 1986, the Web had not yet been invented and cell phones were large clunky objects that few people owned. Since then, technological advancements have transformed the way Americans communicate. Electronic forms of communication are used for virtually every type of private exchange, from sharing personal advice and sending love letters to discussing medical ailments and conveying confidential business information.

Electronic communications are not just augmenting postal mail and the telephone, they are replacing them. Nearly all Americans on the Internet send or read email, and almost 60% do so at least once a day.[5] Moreover, 80% of Americans with cell phones use their devices to send text messages.[6] And postal mail volume has plummeted dramatically over the last few years. The volume of private, personal correspondence has fallen even more sharply than the overall mail volume.[7]

Evidence shows that as the majority of Americans have begun to replace older forms of communication like postal mail and landline telephones with electronic communications, they have tried to bring many of their old privacy practices with them. Email accounts have passwords to make sure no one can read messages without authorization, just as envelopes are

---

[4] *United States v. Jones*, 132 S. Ct. 945, 963-64 (2012) (J. Alito, concurring).
[5] Kristen Purcell, Pew Internet & American Life Project, *Search and email still top the list of most popular online activities*, Aug. 9 , 2011, http://www.pewinternet.org/Reports/2011/Search-and-email.aspx
[6] Joanna Brenner, Pew Internet & American Life Project, *Pew Internet: Mobile*, Jan. 31, 2013, http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx
[7] United States Postal Service. "Facts and figures about your Postal Service 2013." available at: http://about.usps.com/who-we-are/postal-facts/welcome.htm#H2

sealed to give letters the same protection. It is considered highly invasive for one person to read through another's text messages without permission, and many cell phones have the ability to be locked with a code to prevent just that.[8] American cell phone users are worried about privacy: more than half of mobile app users have uninstalled or avoided a cell phone app due to privacy concerns.[9] But despite these clear expectations, ECPA arguably authorizes the government to access many of these private, password-protected communications without obtaining a probable cause warrant, something that would certainly be needed to access the very same messages if they had been sent through an older medium like a written letter or a landline telephone.

This distinction arises in spite of the fact that ECPA contemplates warrants for the content of communication. However, changes in how electronic communications are stored and provided over the years have eroded that protection. When ECPA was written in 1986, users stored their communications on third party servers only briefly. They then downloaded these messages onto their personal computers, where it enjoyed Fourth Amendment protection, and the third party did not keep a copy. ECPA was created with this reality in mind: under the statute, the government may obtain opened emails that are left on servers and unopened emails left on servers for more than 180 days, without a warrant, having only to establish that the messages are "relevant and material" to an ongoing criminal investigation. The rationale for this lower standard was that these emails were the equivalent of abandoned property and hence should be treated like any other business record.

However today, few people download their email onto their own computers. The market has been overtaken by webmail applications provided by companies like Yahoo and Google, where email is stored continuously by third parties. Leaving mail on a server allows you to access your email from other multiple locations, whether home, work, a coffee shop, etc. In addition, many people are increasingly storing their emails for extended periods of time rather than deleting them. ECPA has not been updated to account for these changes in technology and the result is that the government is now arguing that it is entitled to many communications on a standard that common sense and some courts suggests does not satisfy the Constitution.[10]

Similarly antiquated technical distinctions underpin another part of ECPA, the protections for so-called 'remote computing services' (RCS). RCSs provide to the public "computer storage or processing services" and under ECPA that information can be access with a subpoena. In 1986, the only companies providing such services were payroll providers and other companies that handle business records, so a subpoena seemed analogous. Today, companies that provide storage have become the digital equivalent of desk drawers, storing photos, letters,

[8] In a recent survey, 12% of cell phone owners said that another person had accessed their cell phone "in a way that made them feel that their privacy had been invaded." For the 18-24 year old age group, that number jumps to almost a quarter of cell users. Jan Lauren Boyles, Aaron Smith, and Mary Madden, Pew Internet & American Life Project, *Privacy and Data Management on Mobile Devices*, Sep. 5, 2012, http://www.pewinternet.org/Reports/2012/Mobile-Privacy/Key-Findings.aspx

[9] Id.

[10] *Warshak*, at 282.

diaries and every type of sensitive electronic communication. It is clear that these types of communications are equally deserving of a warrant.[11]

In short, the law has not kept pace with technological change. Americans now communicate electronically, and they do so with the expectation that communication can still be private. And, they are right to have that expectation because they should have the same privacy in new technology as they had with old.

Electronic Communications and Location Tracking

In 1986, very few Americans owned a cell phone. Today around 85% of American adults have a cell phone, and many carry their cell phones with them almost everywhere they go.[12] In fact, almost a third of cell phone users describe their cell phone as "something I can't imagine living without."[13]

Although the primary purpose of a cell phone is to make phone calls, a side effect of that communication is the transmission of location information. For the many Americans that travel with and use their cell phones throughout the day, these devices are more than just phones; they are also trackers constantly logging location, often with enough accuracy to pinpoint a particular address.[14] Creation of location information is an inevitable byproduct of this technology: phones must constantly communicate with cell towers in order to make and receive calls. Communications to those towers can in turn be used to determine location. With the increasing use of smart phones, location determination can also be made in a wide variety of other ways including by activating GPS devices in the phones and logging where phones accessed fixed wi-fi hotspots.

The practical result is that law enforcement officers and government officials have the ability to find out exactly where a person was at a given time, or to find out where he or she is in real-time, as long as the person in question carries a cell phone. In addition to tracking individuals, this technical capacity also allows law enforcement to discover every individual who is in the range of a particular cell tower at a particular time. In fact, requests by law enforcement to phone companies are very common and more than 1.3 million such requests took place in 2011 alone.[15]

---

[11] For more on the history of the technology that shaped ECPA please see Orin S. Kerr, A USER'S GUIDE TO THE STORED COMMUNICATIONS ACT, AND A LEGISLATOR'S GUIDE TO AMENDING IT, 72 Geo. Wash. L. Rev. 1208.

[12] Aaron Smith, Pew Internet & American Life Project, *The Best (and Worst) of Mobile Connectivity*, Nov. 30, 2012, http://pewinternet.org/Reports/2012/Best-Worst-Mobile.aspx

[13] Id.

[14] *Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. (2010) (statement of Professor Matt Blaze at 5), *available at* http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf; Thomas Farely & Ken Schmidt, Cellular Telephone Basics: Basic Theory and Operation (2006), http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/

[15]

Location tracking enables law enforcement to capture details of someone's movements for months on end, unconstrained by the normal barriers of cost and officer resources. In a concurrence in the recent Supreme Court case, *U.S. v. Jones*, Justice Sonia Sotomayor described why this was so problematic, emphasizing the intimate nature of the information that might be collected by the GPS surveillance, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[16]

While even the limited collection of geolocation information can reveal intimate and detailed facts about a person, the privacy invasion is multiplied many times over when law enforcement agents obtain geolocation information for prolonged periods of time. As the D.C. Circuit Court of Appeals has observed, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[17]

In addition, there have always been facets of American life that have been uniquely safeguarded from the intrusive interference and observation of government. Geolocational surveillance threatens to make even those aspects of life an open book to government. As Justice Sotomayor pointed out in *Jones*, "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[18]

Finally, while the government routinely argues that records of a person's prior movements deserve less privacy protection than records of where a person travels in real time, this is a meaningless distinction. As one judge has noted, "[t]he picture of [a person]'s life the government seeks to obtain is no less intimate simply because it has already been painted."[19] A contrary conclusion would eliminate privacy protections even in real-time data, because police officers would be free to use GPS devices to record vehicles' travels so long as they waited some minutes before accessing those records, thereby rendering them "historical."

<u>Reporting, Oversight, and Remedies</u>

While protecting the content of electronic communications and location records are crucial elements of ECPA reform, other parts of the law also need to be improved. Specifically, we urge the committee to explore the following additional elements in any ECPA reform proposal:

---

[16] *United States v. Jones*, 132 S. Ct. 945, 955 (2012).
[17] *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010)
[18] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quotations omitted).
[19] *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D.Tex. 2010) (citation omitted).

1. **Institute Appropriate Oversight and Reporting Requirements**. Because electronic record keeping enables easy collection and aggregation of records, current low standards under ECPA allow the government to engage in a largely unsupervised and unreported "shopping spree" through the treasure trove of personal information held by private companies. To ensure adequate oversight by Congress and adequate transparency to the public, existing reporting requirements for wiretap orders must be extended to all types of law enforcement surveillance requests.

2. **Require a Suppression Remedy**. If a law enforcement official obtains non-electronic information illegally, that information usually cannot be used in a court of law. The same rule, however, doesn't apply to illegally-obtained electronic information. Such a rule only encourages government overreaching and must be changed to require a judge to bar the use of such unlawfully obtained information in court proceedings.

3. **Craft Reasonable Exceptions.** Overbroad exceptions are also depriving Americans of their rightful privacy protection. Currently ECPA sometimes allows access to the content of communications without a true emergency, without informed consent, and without prompt notice to the subject. ECPA must be amended on each of these fronts if electronic records are to receive the protections Americans need.

Conclusion

We applaud the Committee for holding this hearing and for undertaking the task of reforming ECPA. Comprehensive reform of ECPA is a needed legislative initiative that will help preserve our fundamental liberties even as the technologies that underpin our lives change. For additional information on ECPA reform or communications privacy please contact ACLU Legislative Counsel Chris Calabrese at 202 715 0839, ccalabrese@dcaclu.org.