KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of James X. Dempsey
Vice President for Public Policy
Center for Democracy & Technology

before the Senate Committee on the Judiciary

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: PROMOTING SECURITY AND PROTECTING PRIVACY IN THE DIGITAL AGE

September 22, 2010

Chairman Leahy, Ranking Member Sessions, Members of the Committee, thank you for the opportunity to testify today.

Introduction and Overview

Justice Brandeis famously called privacy "the most comprehensive of rights, and the right most valued by a free people." The Fourth Amendment embodies this right, requiring a judicial warrant for most searches or seizures,[1] and Congress has enacted numerous laws affording privacy protections going beyond those mandated by the Constitution.

In setting rules for electronic surveillance, the courts and Congress have sought to balance two critical interests: the individual's right to privacy and the government's need to obtain evidence to prevent and investigate crimes, respond to emergency circumstances and protect the public. More recently, as technological developments have opened vast new opportunities for communication and commerce, Congress has added a third goal: providing a sound trust framework for communications technology and affording companies the clarity and certainty they need to invest in the development of innovative new services.

Today, it is clear that the balance among these three interests – the individual's right to privacy, the government's need for tools to conduct investigations, and the interest of service providers in clarity and customer trust – has been lost as powerful new technologies create and store more and more information about our daily lives. The protections provided by judicial precedent and statute have failed to keep pace, and important information is falling outside the traditional warrant standard.

[1] "Warrantless searches are presumptively unreasonable, though the Court has recognized a few limited exceptions to this general rule." United States v. Karo, 468 U.S. 705, 717 (1984).

Two major developments in technology in the past ten years stand out:

- "Cloud computing," which is the use of Internet-based resources for the storage and processing of all kinds of information. More and more private and proprietary information is moving off the desktop or laptop computer and out of our homes and offices onto the computers of service providers, which store the information, protect it, and make it available pursuant to the instructions of the owner of the information.

- The revolution in mobile communications and the associated development of location-based services. Nearly 300 million Americans rely in their business and personal lives on cell phones and other mobile devices, which generate information locating the individual every few seconds.

Under the Electronic Communications Privacy Act of 1986, neither private information stored in the cloud nor location tracking information is accorded the traditional protection of the judicial warrant. According to ECPA, private documents stored in the cloud, including all our email more than 180 days old as well as documents regardless of age, are available to government investigators without a warrant, even though it would require a warrant to immediately seize the very same material directly from the party who created it. Likewise, ECPA does not specify that a warrant is required for the government to track our location through our cell phones. The courts, as they often have been in the past, are being slow in responding to these technological changes.

The personal and economic benefits of technological development should not come at the price of privacy. In the absence of judicial protections, it is time for Congress to respond, as it has in the past, to afford adequate privacy protections, while preserving law enforcement tools and providing clarity to service providers.

A Brief History of Electronic Surveillance Law

The history of privacy in America is characterized by the recurring efforts of courts and Congress to catch up with technology.

In 1878, the Supreme Court stated in *Ex parte Jackson*, 96 U.S. 727, that the Fourth Amendment applied to sealed letters while in the possession of the Post Office. Even though the letter was voluntarily placed in the hands of a third party, the Court concluded, it was still protected by the Constitution and could not be read without a warrant.[2]

In 1928, however, in *Olmstead v. United States*, 277 U.S. 438, the Supreme Court held that a telephone conversation was not protected by the Fourth Amendment if it was intercepted from the facilities of the service provider. The *Olmstead* Court concluded, in essence, that users of the telephone voluntarily surrendered the privacy of their communications by disclosing them to the telephone company: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment." 277 U.S. at 466.

[2] "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be." 96 U.S. at 733.

Justice Brandeis, in his famous dissent, said that the majority opinion was inconsistent with the Court's earlier ruling on the privacy of letters. Quoting the lower court, Brandeis said, "There is, in essence, no difference between the sealed letter and the private telephone message. … 'True, the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed; but these are distinctions without a difference.'" *Id.* at 475. Justice Brandeis criticized the Court's focus on physical trespass and warned that technology would continue to change in ways that would erode privacy if the law remained static: "The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." Id. at 474.

In 1934, when Congress adopted the Communications Act, it responded to the Olmstead decision by making it illegal for any person to "intercept … and divulge or publish" the contents of any wire communication. Over succeeding decades, the courts and the Justice Department tussled over the interpretation of Section 605. The Justice Department argued, for example, that its agents were not "persons" under the Act. The Supreme Court rejected that theory. Nardone v. United States, 302 U.S. 379 (1937). The Justice Department nevertheless proceeded to wiretap on the theory that it was legal to do so under Section 605 so long as it did not divulge the intercepts outside law enforcement.

It took 40 years for a Court majority to settle the issue and acknowledge Justice Brandeis' call for technology neutrality in the application of the Fourth Amendment. Finally, in *Katz v. United States*, 389 U.S. 347 (1967), Justice Stewart wrote that the "Fourth Amendment protects people, not places. … [What a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." The Court based its decision in part on the fact that the telephone had come to play a central role in everyday life. *Id.* at 352 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

Next it was Congress' turn again. To implement the Constitutional ruling of *Katz* and the related case on bugging, *Berger v. New York*, 388 U.S. 41 (1967), Congress in 1968 adopted the federal Wiretap Act, 18 U.S.C. 2510 *et seq*., establishing detailed procedural rules for obtaining judicial warrants to carry out wiretaps. The statute provided many details the courts would not have been well-suited to develop.[3] Congress, however, forgetting Justice Brandeis' prediction about the steady progress of technology, only covered voice communications carried over a wire and face-to-face oral conversations.

After *Katz*, the pace of technological change accelerated dramatically. By the 1980s, two forms of communications were emerging that did not fit well within the definitions of the Wiretap Act: Wireless telecommunications were emerging in the form of early cellular phones, and the modem was making it possible to transmit non-voice data over the telephone system. The rationale of *Katz* would seem to suggest that wireless and data communications were just as much protected by the Fourth Amendment as wireline, voice calls. However, there were arguments, harking back to *Olmstead*, that cell phone users surrendered their privacy when they voluntarily used a service that went over the air. Similarly, decisions of the Supreme Court holding that there was no privacy right in some kinds of records stored with a third party cast a

[3] See Orin S. Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004).

shadow of doubt over the status of Internet communications, which were stored on network computers as they hopped from node to node and before they were accessed by their intended recipients.

Congress concluded that it would be unwise to wait for cases resolving the status of these emerging technologies to percolate up through the courts. After all, it took decades for the Supreme Court to extend the Fourth Amendment to the telephone. The fledgling wireless and Internet industries wanted to be able to assure potential customers that their communications were private. Key policymakers – led in the Senate by the present Chairman of this Committee -- foresaw the potential of these technologies, in terms of both economic development and human interaction. Another *Olmstead* would have been devastating to privacy and innovation. To remove the cloud of doubt about privacy, and in order to provide a sound footing for investment and innovation, Congress adopted the Electronic Communications Privacy Act of 1986.

The stated goal of ECPA was twofold: 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), and to support 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).

ECPA updated the Wiretap Act by specifying that a judicial warrant was required for the "interception" of wireless communications and data communications – that is, the monitoring of cellular calls and email in real-time, as they were being transmitted. ECPA also specified that the government needed a warrant to compel a service provider to disclose the content of email it was holding in electronic storage – but only up to a point. In 1986, Congress assumed that users would access their email accounts periodically and download their email onto their personal computers. The service providers would then delete the email from their servers. Congress thought that the longest conceivable time that any service provider would keep email would be 6 months. So Congress provided that a warrant was required only for access to email 180 days old or less. After 180 days, the account was assumed to be abandoned and the service provider could be compelled with a mere subpoena to turn over anything it still had.

ECPA also set standards for use of pen registers and trap trace devices to intercept dialed number information. The Supreme Court had ruled that telephone users had no privacy interest in the dialing information associated with their phone calls. Congress reacted by requiring a court order for live interception of dialing information, but it set a very low standard, specifying that the courts "shall" approve all government requests certifying that the information likely to be obtained is relevant to an ongoing investigation. ECPA also authorized use of subpoenas to compel disclosure of subscriber identifying information and stored transactional records.

Changes in Technology Have Outpaced ECPA

While ECPA was a forward-looking statute when enacted in 1986, technology has advanced dramatically since 1986, and the statute has been outpaced. While there have been many small amendments to ECPA, the statute has not undergone a significant review since it was enacted in 1986 – light years ago in Internet time. ECPA today is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for many service providers and law enforcement agencies alike. Moreover, it provides inadequate protection for huge amounts of personal information.

Since enactment of ECPA, there have been fundamental changes in communications technology and the way people use it, including –

- **Email**: Most Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Because of the importance of email and unlimited storage capabilities available today, most people save their email indefinitely, just as they previously saved letters and other correspondence. The difference, of course, is that it is easier to save, search and retrieve digital communications. Many of us now have many years worth of stored email. Moreover, for many people, much of that email is stored on the computers of service providers.[4] **However, ECPA provides only weak protection for stored email that is more than 180 days old, allowing governmental access without a warrant. Moreover, the Justice Department argues that email loses the protection of the warrant the instant the sender sends it and, on the other end, the minute the recipient accesses it or opens it.**

- **Mobile location:** Cell phones and mobile Internet devices constantly generate location data that supports both the underlying service and a growing range of location-based services of great convenience and value. This location data can be intercepted in realtime, and is often stored in easily accessible logs files. Location data can reveal a person's movements, from which inferences can be drawn about their activities and associations and their presence in homes and other private palces. **ECPA does not clearly specify a standard for government access to cell phone location information, and agents have been obtaining it without a warrant.** See Michael Isikoff, The Snitch in Your Pocket, Newsweek (Feb. 19, 2010) http://www.newsweek.com/id/182403.

  Most significantly, the precision with which cell phones can be located using cell site data has been steadily improving, as carriers build out their networks with cells covering smaller and smaller areas, so that today cell site location information is sometimes as precise as GPS. As Prof. Matt Blaze of the University of Pennsylvania explained in testimony before a House subcommittee earlier this year, "The effect of this trend toward smaller sectors is that knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic

[4] For example, Google's Gmaillll service offers more than seven gigabytes of free storage space. Google, *Google Storage*, *available at* http://mail.google.com/support/bin/answer.py?hl=en&answer=39567 (visited Mar. 30, 2010). Google actually encourages its users not to delete their messages from Google's computers. Google, *Getting Started with Gmail*, *available at* http://mail.google.com/mail/help/intl/en/start.html (visited Mar. 30, 2010) ("Don't waste time deleting . . . . [T]he typical user can go years without deleting a single message.").

area. In relatively unpopulated areas with open terrain, this may be an area miles in diameter. But in urban areas and other environments that use microcells, this area can be quite small indeed, sometimes effectively identifying individual floors and rooms within buildings."[5] Consequently, Blaze concluded, the distinction between cell site location data and GPS data "is increasingly obsolete, and as cellular networking technology evolves, it is likely to become effectively meaningless. As microcell technology and enhanced location techniques become more widely deployed in cellular networks, the information revealed though the cell sector identifier pinpoints, under many circumstances, a user's location to a degree once possible only with dedicated GPS tracking devices."

- **Cloud computing**: Increasingly, businesses and individuals are storing data "in the cloud," with potentially huge benefits in terms of cost, security, flexibility and the ability to share and collaborate. **ECPA needs to be amended to clarify that data stored and processed in the cloud has the same protections and standards for law enforcement access as data stored locally.**

- **Social networking:** One of the most striking developments of the past few years has been the remarkable growth of social networking. Hundreds of millions of people now use these social media services to share information with friends and as an alternative platform for private communications. **Even when private records, photos and other materials are shared only with a couple of friends, ECPA may provide only weak protection, allowing governmental access without a warrant.**

- **Tracking and logging of online activity:** For a variety of reasons, Internet service providers, websites and other online service providers collect and log detailed information about online activity. While many Internet users have a perception of anonymity, in fact much of what they do online can be personally tied to them through their computer addresses and other information disclosed and logged in the ordinary course of using the Internet. ECPA authorizes a subpoena to acquire certain types of subscriber identifying information. **However, government agencies have been filing blanket subpoenas seeking to identify all individuals who visited a particular site containing lawful content or all users of a legitimate online service.**

In the face of these developments, ECPA does not provide protection suited to the way technology is used today:

- **Conflicting standards and illogical distinctions:** ECPA sets rules for governmental access to email and stored documents that are not consistent. A single email is subject to multiple different legal standards in its lifecycle. See Appendix A. To take another example, a private document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but DOJ argues under ECPA that the same document stored with a service provider is not be subject to the warrant requirement.

- **Unclear standards:** ECPA does not clearly state the standard for governmental access to location information. In the past 5 years, no fewer than 30 federal opinions have been

[5] Testimony of Prof. Matt Blaze, House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services, June 24, 2010, http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf.

published on government access to cell phone location information, reaching a variety of conclusions.

- **Judicial criticism:** The courts have repeatedly criticized ECPA for being confusing and difficult to apply. The Ninth Circuit in 2002 said that Internet surveillance was "a confusing and uncertain area of the law."[6] The Third Circuit last month complained that, in trying to determine what standard was appropriate for cellphone tracking, "we are stymied by the failure of Congress to make its intention clear."[7]

The Courts Are Unlikely to Resolve Soon The Questions Posed By New Technology

It appears unlikely that the courts will anytime soon resolve these issues on Constitutional grounds. The courts have been progressing sporadically and inconclusively in assessing the application of the Fourth Amendment to stored email. When a panel of the Sixth Circuit ruled that stored email was protected by the Constitution, an en banc panel vacated the opinion on ripeness grounds. Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), vacated en banc, 532 F.3d 521 (2008). Conversely, in March of this year a panel of the Eleventh Circuit held that stored email was *not* protected by the Constitution, Rehberg v. Paulk, 598 F.3d 1268, and in July the same judges vacated that opinion and substituted for it one holding that, if the Fourth Amendment right existed, it wasn't "clearly established."[8] The Ninth Circuit held in 2008 that the Constitution protected stored text messages, Quon v. Arch Wireless, 529 F.3d 892 (2008). The Supreme Court this summer reversed the Ninth Circuit, but it did so without ruling on the question of whether the Fourth Amendment protects stored text messages. City of Ontario v. Quon. Instead the Court assumed arguendo that there was a reasonable expectation of privacy. The Court emphasized that it was reluctant to "elaborate too fully on the Fourth Amendment implications of emerging technology."

Similarly, the courts have been unable to resolve questions about the Constitutional status of location tracking information. Last month, within a week's time, the D.C. Circuit held that prolonged GPS tracking was a search under the Fourth Amendment, United States v. Maynard, and the Ninth Circuit held that it was not, United States v. Pineda-Moreno. And three weeks after that, the Third Circuit held that ECPA gives magistrates the option of requiring a warrant to obtain cell site location information. Meanwhile, there have been about three dozen opinions by federal magistrates and district court judges on a variety of cell phone tracking questions, with a variety of outcomes although, by our count, a majority of those dealing with real-time tracking have held that a warrant is necessary.

This murky legal landscape does not serve the government, customers or service providers well. Customers are, at best, confused about whether their data is subject to adequate protections when the government seeks access. Companies are uncertain of their responsibilities and unable to assure their customers that subscriber data will be uniformly protected. The current state of the law does not well serve law enforcement interests either, as resources are wasted on litigation over applicable standards and prosecutions are in jeopardy

---

[6] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

[7] In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, No. 08-4227 (3d Cir. Sept. 7, 2010).

[8] http://www.ca11.uscourts.gov/opinions/ops/200911897reh.pdf.

should the courts ultimately rule on the Constitutional questions. The solution is a clear set of rules for law enforcement access that will safeguard end-user privacy, provide clarity for service providers, and enable law enforcement officials to conduct effective and efficient investigations.

The Digital Due Process Coalition

For nearly three years, privacy advocates, legal scholars, and major Internet and communications service providers have been engaged in a dialogue to explore how ECPA applies to new services and technologies. The Center for Democracy & Technology chaired those discussions. Earlier this year, those discussions reached a milestone when a diverse coalition developed consensus around a core set of principles for updating ECPA. The principles are open for signature and new entities are continuing to endorse it. The coalition so far includes Amazon.com, AOL, AT&T, CCIA, Data Foundry, eBay, Facebook, Google, Hewlett-Packard, IAC, Integra Telecom, Intel, Linden Lab, Loopt, Microsoft, NetCoalition, Qwest, Salesforce.com, TIA and TRUSTe, as well as the ACLU, the Electronic Frontier Foundation, FreedomWorks, Americans for Tax Reform, and the Competitive Enterprise Institute. See Appendix B for a full list of Coalition members.

The coalition did not seek to answer all questions or concerns about ECPA. Though members of the coalition may differ on the specifics, and some individual members would support additional changes, all agreed on four principles that provide a framework for opening a public dialogue on the issue. This is what the coalition reached consensus on:

> ***Updating The Electronic Communications Privacy Act of 1986***
>
> ***Overarching goal and guiding principle:*** *To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.*
>
> *These principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA:*
>
> 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.*

In this written testimony and in my oral remarks, I speak only on behalf of CDT. I do not speak for the coalition or any of its other members. However, I draw extensively on a background memo prepared by the coalition. The full consensus text of the DDP memo is online at http:/www.digitaldueprocess.org. In addition, the site includes a lengthy analysis by J. Beckwith Burr of WilmerHale.

The overarching goal of ECPA reform should be to balance the law enforcement interests of the government, the privacy interests of users, and the interests of communications service providers in certainty, efficiency and public confidence. In addition, the following concepts should guide any reform:

- **Technology and Platform Neutrality**: A particular kind of information (for example, the content of private communications) should receive the same level of protection regardless of the technology, platform or business model used to create, communicate or store it.[9]

- **Assurance of Law Enforcement Access**: The reform principles would preserve all of the building blocks of criminal investigations – subpoenas, court orders, pen register orders, trap and trace orders, and warrants – as well as the sliding scale that allows the government to escalate its investigative efforts.

- **Equality Between Transit and Storage**: Generally, a particular category of information should be afforded the same level of protection whether it is in transit or in storage.

- **Consistency**: The content of communications should be protected by a court order based on probable cause, regardless of how old the communication is and whether it has been "opened" or not.

- **Simplicity and Clarity**: All stakeholders – service providers, users and government investigators – deserve clear and simple rules.

- **Recognition of All Existing Exceptions**: Over the years, a variety of exceptions have been written into the ECPA, such as provisions allowing disclosures to the government without court orders in emergency cases. These principles should leave all those exceptions in place.

Rather than attempt a full rewrite of ECPA, which might have unintended consequences, it is best to focus just on the most important issues – those that are arising daily under the current

[9] Technology neutrality is a principle to be applied with caution. For example, design mandates developed for the traditional telephone network would not be suited to Internet technologies.

law: access to email and other private communications stored in the cloud, access to location information, and the use of subpoenas to obtain transactional data.

What Would ECPA Reform Mean in Practice

The Digital Due Process recommendations preserve the "building blocks" of criminal investigations. Under current law, government investigators often work their way up the ladder to probable cause, starting with subpoenas for subscriber identifying information and stored transactional data, then moving to court orders under 2703(d) for more detailed transactional data and court orders, based on less than probable cause, for real-time interception of signaling and routing information. Based on analysis of this and other data, they may then have probable cause to obtain a search warrant. The DDP recommendations preserve all these building blocks of the investigative process.

Stored Communications and Private Documents: The first principle endorsed by the DDP coalition is that the government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online.

- This principle applies to private communications, documents and other private user content stored in or transmitted through the Internet "cloud" the same warrant standard that the Constitution and the Wiretap Act have traditionally provided for the privacy of our phone calls or the physical files we store in our homes. It is intended to apply to private emails, instant messages, text messages, word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks. It is not intended to apply to materials revealed to the public on the Internet.

- This change was first proposed in bi-partisan legislation introduced in 1998 by Senators John Ashcroft and Patrick Leahy. It is consistent with recent Appeals Court decisions holding that emails and SMS text messages stored by communications providers are protected by the Fourth Amendment, and is also consistent with the latest legal scholarship on the issue.

Location Tracking: The second DDP reform principle states that the government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.

- This principle addresses the treatment of the growing quantity and quality of data based on the location of cell phones, laptops and other mobile devices, which is currently the subject of conflicting court decisions; it proposes the conclusion reached by a majority of the courts that a search warrant is required for real-time cell phone tracking, and would apply the same standard to access to stored location data.

- Many details of this principle would have to be worked through, including the definition of location information, the exceptions that would be recognized (which would certainly have to include emergency circumstances), and the relationship between requests for location information and requests for other call detail records and subscriber identifying information.

- A warrant for mobile location information was first proposed in 1998 as part of the bipartisan Ashcroft-Leahy bill. The House Judiciary Committee in 2000 reported by a 20-1 vote legislation that would have required a warrant for real-time tracking of mobile phones.

Access to Transactional Data: Under the DDP's third principle, before obtaining transactional data in real time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation.

- In 2001, the law governing "pen registers and trap & trace devices"—technologies used to obtain transactional data in real time about when and with whom individuals communicate over the phone—was expanded to also allow monitoring of communications made over the Internet. In particular, the data at issue includes information on who individuals email with, who individuals IM with, who individuals send text messages to, and the Internet Protocol addresses of the Internet sites individuals visit.

- This principle would update the law to reflect modern technology by establishing judicial review of surveillance requests for this data based on a factual showing of reasonable grounds to believe that the information sought is relevant and material to a crime being investigated.

Overbroad Subpoenas: Finally, before obtaining transactional data about multiple unidentified users of communications or other online services when trying to track down a suspect, the government should first demonstrate to a court that the data is needed for its criminal investigation.

- This principle addresses the circumstance when the government uses subpoenas to get information in bulk about broad categories of telephone or Internet users, rather than seeking the records of specific individuals that are relevant to an investigation. For example, there have been reported cases of bulk requests for information about everyone that visited a particular web site on a particular day, or everyone that used the Internet to sell products in a particular jurisdiction.

- Because such bulk requests for information on classes of unidentified individuals implicate unique privacy interests, this principle applies a standard requiring a showing to the court that the bulk data is relevant to an investigation.

What the Digital Due Process Principles Would Not Do

In the view of CDT, the recommendations endorsed by the Digital Due Process coalition are quite modest and would have minimal adverse impact on law enforcement investigations while providing important privacy protections.

- They would not affect FISA or the National Security Letter authority of ECPA (18 U.S.C. 2709).

- They would not affect emergency disclosures. The Wiretap Act, the Stored Communications Act, and the pen register/trap and trace provisions all contain emergency exceptions that permit interceptions and service provider disclosure without a warrant (and even without a subpoena). The principles offered by the DDP would not affect any of these emergency disclosures. The warrant requirement for access to location information recommended by DDP would have to be subject to similar emergency exceptions. Calls to 911 would also be exempted from the warrant requirement, under both the consent principle and the emergency exception.

- The principles would not affect cybersecurity. Service providers currently have broad authority to monitor their own networks for cybersecurity purposes and to disclose to the government information about suspected attacks or intrusions. The DDP recommendations would not alter these authorities.

- They would have zero impact on child pornography, child abuse and child safety investigations. The principles were carefully crafted to preserve fully the tools critical to these investigations. They do not alter in any way the child pornography reporting provisions in federal and state law. They do not alter the exceptions or other permissions granted in the statute for providing information to the government in child abduction cases. They do not alter any authority that service providers have to monitor their systems for child abuse images and to disclose such images to NCMEC or law enforcement.

- The recommendations would not cover anything publicly disclosed on the Internet. Moreover, they would not stop a police officer from "friending" someone on Facebook and obtaining access to otherwise private communications. The rules permitting undercover operations and other deceptive techniques would remain unaffected.

- The recommendations, like ECPA itself, focus on compulsory access from service providers. The recommendations would not change the rules for voluntary disclosure by the customers of those service providers. Nor do the recommendations change the rules for use of subpoenas served on the sender or recipient of an email or the creator of a document. The rule applicable to postal mail would also apply to email: the recipient of an email, like the recipient of a letter, could voluntarily disclose that email to the government and could be compelled to disclose it with a subpoena. The sender of an email could be compelled to disclose it with a mere subpoena to the same extent that the sender of a letter can be compelled to disclose a retained copy. If the creator of a document could be compelled with a subpoena to disclose it, under the DDP principles the creator could be compelled to disclose whether the document was stored locally or in the cloud.

Disclosure to a Third Party Does Not Destroy a Privacy Interest

The ECPA reform proposals here are consistent with the long line of cases holding that individuals have privacy rights in materials that they entrust to third parties and in spaces rented from third parties. As noted above, the Supreme Court has recognized a Constitutional expectation of privacy in the contents of sealed packages and letters, even when those letters and packages are voluntarily given to the government-run Post Office. *Ex Parte Jackson*, 96 U.S. 727, 733 (1878). Bank customers have a privacy interest in the contents of their safe

deposit boxes, requiring a warrant for government access. *United States v. Thomas*, No. 88-6341, 1989 WL 72926, at *2 (6th Cir. July 5, 1989). Moreover, this privacy right survives even if the service provider has rights to enter the protected space or inspect the material. Tenants in rented residences and hotel rooms maintain Fourth Amendment privacy rights in their units. *Stoner v. California*, 376 U.S. 483, 489 (1964). The fact that landlords and hotel managers may be entitled to enter the premises for maintenance and other purposes does nothing to diminish the tenants' expectations against the government. *Id.*

The Wiretap Act recognizes the same principle. It permits service providers to conduct service quality monitoring and to examine and disclose customer communications for the purpose of protecting the rights and property of the service provider. None of these actions diminish the privacy right of the telephone customer as against governmental intrusion, nor should the activities of providers of free Internet email and free cloud computing services diminish the privacy rights of users as against others.

Other ECPA Issues May Deserve Attention

There are other issues that may merit attention in addition to those covered by the consensus principles of the Digital Due Process coalition.

- Civil litigant access. Several court decisions have made it clear that ECPA does not allow civil litigants to compel the disclosure of communications by electronic communications service providers or providers of remote computing service to the public; under these rulings, such requests should be served on the sender or recipient of the communications who can be compelled under normal discovery rules to either retrieve them and disclose them to the litigant or to give consent to the service provider to disclose them. While these cases are a correct reading of ECPA, and while they offer a clear path to discovery in most cases, service providers continue to spend considerable resources defending against civil litigant requests, briefing the issue one court at a time. Some have argued that ECPA could be clarified, while perhaps including a safety valve process for cases in which the user whose communications are sought cannot be found.

- Reporting and transparency. The Wiretap Act requires annual publication of statistics on wiretapping, but there is no comparable requirement for pen register and trap and trace devices or for compulsory disclosure of stored content.

- The Wiretap Act only covers interception of communications. It does not cover the use of video cameras in private places. The recent case in Marion County, PA, in which a school turned on the cameras in computers issued to students and took pictures of the students engaging in a variety of activities inside their homes, highlighted this gap in the law. See Testimony of Kevin Bankston before the Senate Judiciary Committee, Subcommittee on Crime and Drugs (March 29, 2010) http://www.eff.org/files/bankston_video_surveillance_testimony.pdf.

Conclusion

In just the past 5 to 10 years, entrepreneurs have developed and the American public has embraced truly revolutionary changes in communications and information technology. These

changes have yielded remarkable benefits in terms of economic activity, education, democratic participation and support for friendships and family relationships. Further amazing developments are surely on the way. Our economic recovery depends in large part on innovation in information and communications technologies.

These benefits should not come at the price of privacy. Nor should privacy concerns be allowed to discourage further innovation. As it has in the past, Congress should update the privacy laws to preserve the balance between government power and personal privacy, preserving law enforcement tools and giving companies the clarity they deserve. Congress should extend the traditional warrant standard to our personal communications, private documents and highly sensitive information like mobile tracking data. Other less sensitive data should be available with a subpoena, so long as the government cannot make blanket requests without judicial approval. These changes would provide the framework for further innovation and growth.

Appendix A

One Email - Multiple Different Standards

ECPA, as interpreted by the Justice Department and the courts, provides a patchwork quilt of standards for governmental access to email. Under ECPA today, the status of a single email changes dramatically depending on where it is stored, how old it is, and even the district within which the government issues or serves its process.

Standards for access to the content of an email:

- Draft email stored on desktop computer – As an email is being drafted on a person's computer, that email is fully protected by the Fourth Amendment: the government must obtain a search warrant from a judge in order to seize the computer and the email.

- Draft email stored on gMail – However, if the person drafting the email uses a "cloud" service such as Google's gMail, and stores a copy of the draft email with Google, intending to finish it and send it later, ECPA says that Google can be compelled to disclose the email with a mere subpoena. 18 U.S.C. 2703(b).

- Content of email in transit – After the person writing the email hits "send," the email is again protected by the full warrant standard as it passes over the Internet. Most scholars and practitioners assume that the Fourth Amendment applies, but in any case the Wiretap Act requires a warrant to intercept an email in transit.

- Content of email in storage with service provider 180 days or less – Once the email reaches the inbox of the intended recipient, it falls out of the Wiretap Act and into the portion of ECPA known as the Stored Communications Act, 18 U.S.C. 2703(a). At least so long as the email is unopened, the service provider can be forced to disclose it to the government only with a warrant.

- Content of opened email in storage with service provider 180 days or less – The Justice Department argues that an email, once opened by the intended recipient, immediately loses the warrant protection and can be obtained from the service provider with a mere subpoena. (Under the same theory, the sender of an email immediately loses the warrant protection for all sent email stored with the sender's service provider.) The Ninth Circuit has rejected this argument. The question remains unsettled in the rest of the country. The Justice Department recently sought opened email in Colorado without a warrant; when the service provider resisted, the government withdrew its request, which means in effect that outside of the Ninth Circuit there may be one standard for service providers who comply with subpoenas and one for service providers who insist on a warrant.

- Content of email in storage with service provider more than 180 days – ECPA specifies that all email after 180 days loses the warrant protection and is available with a mere subpoena, issued without judicial approval.

Appendix B
Members of Digital Due Process
(as of September 20, 2010)

Companies

Amazon.com
AOL
AT&T
Data Foundry
eBay
Facebook
Google
Hewlett-Packard
IAC
Integra Telecom
Intel
Linden Lab
Loopt
Microsoft
Qwest
Salesforce.com
TRUSTe

Trade Associations, Thinks Tanks and other Organizations

American Booksellers Foundation for Free Expression (ABFFE)
American Civil Liberties Union (ACLU)
American Library Association (ALA)
Association of Research Libraries (ARL)
Americans for Tax Reform (ATR)
Association of Research Libraries (ARL)
Bill of Rights Defense Committee (BORDC)
Center for Democracy & Thnology (CDT)
Center for Financial Privacy & Human Rights
Citizens Against Government Waste (CAGW)
Competitive Enterprise Institute (CEI)
Computer & Communications Industry Association (CCIA)
The Constitution Project
Consumer Action
Distributed Computing Industry Association (DCIA)
Electronic Frontier Foundation (EFF)
The Future of Privacy Forum
FreedomWorks
Information Technology & Innovation Foundation (ITIF)
NetCoalition
The Progress & Freedom Foundation (PFF)
Telecommunications Industry Association (TIA)