UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

In the Matter of

Information Privacy and Innovation in the Internet Economy **Docket No. 100402174-0175-01**

COMMENTS OF DIGITAL DUE PROCESS

June 14, 2010

In response to the Notice of Inquiry in the above captioned matter, Digital Due Process is pleased to submit the following comments.

Digital Due Process (DDP) is a broad coalition of technology and communications companies, trade associations, advocacy groups, and think tanks, as well as academics and individual lawyers. A full, current list of DDP members appears at the end of this document. On March 30 of this year, DDP issued principles for updating the key federal law that defines the rules for government access to email and private files stored in the Internet "cloud." The coalition effort was prompted by the need to preserve traditional privacy rights in the face of technological change while also ensuring that law enforcement agents can carry out investigations and that industry has the clarity needed to innovate.

To set a consistent standard in line with the traditional rules for law enforcement access in the offline world, the group's recommendations focus on the Electronic Communications Privacy Act (ECPA). Passed in 1986 and not significantly updated since, it establishes standards for government access to email and other electronic communications in criminal investigations.

Technology has changed dramatically in the last 20 years, but the law has not. The traditional standard for the government to search one's home or office and read one's mail or seize one's personal papers is a judicial warrant. The law needs to be clear that the same standard applies to email and documents stored with a service provider, while at the same time be flexible enough to meet law enforcement needs.

The group is reaching out to government officials and anticipates extended dialogue with law enforcement agencies to develop consensus on updates to the law. We urge the Department to join in this process.

ECPA Reform: Why Now?

The Electronic Communications Privacy Act (ECPA) was a forward-looking statute when enacted in 1986. It specified standards for law enforcement access to electronic communications and associated data, affording important privacy protections to

subscribers of emerging wireless and Internet technologies. Technology has advanced dramatically since 1986, and ECPA has been outpaced. The statute has not undergone a significant revision since it was enacted in 1986 – light years ago in Internet time.

As a result, ECPA is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies. ECPA can no longer be applied in a clear and consistent way, and, consequently, the vast amount of personal information generated by today's digital communication services may no longer be adequately protected. Concern about the privacy afforded personal and business information can hold back adoption of emerging technologies, discouraging innovation. ECPA's complexity also imposes substantial costs on service providers seeking to review and comply with data requests from law enforcement. At the same time, ECPA must be flexible enough to allow law enforcement agencies and service providers to work together effectively to combat increasingly sophisticated cyber-criminals or sexual predators.

The time for an update to ECPA is now. For more than a year, 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. We have developed consensus around the notion of a core set of principles intended to simplify, clarify, and unify the ECPA standards; provide clearer privacy protections for subscribers taking into account changes in technology and usage patterns; and preserve the legal tools necessary for government agencies to enforce the laws and protect the public.

The Economic Context for ECPA Reform

Since ECPA was adopted in 1986, the Internet has evolved from a research network with a few thousand academic hosts into a global platform for communications, commerce, and civic activity. According to the most recent Pew survey, an estimated 74% of Americans use the Internet.[1/] Information technology has driven the U.S. economy in the past two decades,[2/] and could, given the proper policy framework, support re-invigoration of the economy for years to come.[3/] The Internet and information technology could be especially important in job creation.[4]

1/ Pew Research Center, "Internet, broadband and cell phone statistics," (January 5, 2010) http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx. However, the fact that Internet usage has remained essentially static since 2006, *id.*, suggests that continued attention is needed to the policy framework supporting Internet expansion.

2/ *See* Robert D. Atkinson & Andrew S. McKay, *Information Technology & Innovation Foundation, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 11-14 (March 2007) ("[T]here is a now a strong consensus among economists that the IT revolution was and continues to be responsible for the lion's share of the post '95 rebound in productivity growth.").

3/ *See id*. at 53 ("Many sectors, such as health care, education, and government, have only begun to tap the benefits of IT-driven transformation. Adoption rates of e-commerce for most consumers, while rapid, are still relatively low. And new technologies (*e.g.*, RFID, wireless broadband, voice recognition) keep emerging that will enable new applications. In short, while the emerging digital economy has produced enormous benefits, the best is yet to come. The job

Cloud computing[5/] is a key element of technological innovation today. Businesses and individuals are now increasingly storing data "in the cloud," with huge benefits in terms of productivity, cost, security, flexibility and the ability to work with collaborators around the world.[6/] More than two-thirds of Internet users use some form of cloud computing service.[7] Cloud computing, "by altering the basic economics of access to computing and storage … has the potential to reshape how U.S. and global businesses are organized and operate."[8/] Most importantly, American tech companies are global leaders in the cloud computing industry today.

---

of policymakers in developed and developing nations alike, is to ensure that the policies and programs they put in place spur digital transformation so that all their citizens can fully benefit from robust rates of growth.").

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

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

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

[7] *Use of Cloud Computing Applications and Services*, Pew Internet & American Life Project, Sep. 12, 2008, Pg. 4, available at http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.

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

The issue of privacy is important to the users of cloud computing. A 2008 study found that 64 percent of American Internet users are concerned about cloud computing companies turning over their files to law enforcement.[9] A survey completed just last week found that a large majority of Americans (88%) believe consumers should enjoy legal privacy protections online similar to those they have offline, while only 4% disagree.[10] Moreover, cloud computing experts warn that potential clients are seeking data storage centers outside the U.S. due to concerns that our laws give the government access to huge quantities of information with little judicial oversight.[11] If this trend continues, American workers may miss out on the jobs that would accompany the growth of this industry.

The use of location information is another trend creating major market opportunities for U.S. companies. There are already a number of innovative, socially beneficial "location aware" applications that employ technologies such as GPS, cell phone infrastructure, or wireless access points to locate electronic devices and provide "resources such as a 'you are here' marker on a city map, reviews for restaurants in the area, a nap alarm triggered by your specific stop on a commuter train, or notices about nearby bottlenecks in traffic."[12/] More applications such as these are emerging every day. A 2010 study forecast that revenues from mobile location-based services could grow to more than $12.7 billion by 2014.[13] However, uncertainty about the privacy afforded location information can hold back consumer use of this technology.[14]

---

people and work together. *See* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf

[9] Id., at p. 7.

[10] Zogby International, Results from June 4-7 Nationwide Poll (June 7, 2010) http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf. According to the survey, the large majority (79%) believes law enforcement should have to get a warrant, like the one they have to get to wiretap phone conversations, to track where a user goes on the Internet, while 12% do not.

[11] Jeffery Rayport and Andrew Heyward, *Envisioning the Cloud: The Next Computing Paradigm*, Marketspace, Mar. 20, 2009, p. 38, available at http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.

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

[13] Robin Wauters, *Mobile Location-Based Services Could Rake in $12.7 Billion by 2014: Report*, TechCrunch, Feb. 23, 2010, http://techcrunch.com/2010/02/23/location-based-services-revenue.

[14] Tsai, et al., *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University (Feb. 2010), p. 18, http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

Changes in Technology Have Outpaced the Law

Justice Brandeis famously called privacy "the most comprehensive of rights, and the right most valued by a free people." Of course, privacy must be balanced against other societal interests. Electronic communications and associated data can provide key evidence in the investigation of many crimes, and the assistance of service providers is often necessary to access such evidence. With respect to communications privacy and law enforcement investigations, the courts and Congress have sought to develop rules for government surveillance that balance three interests: the individual's constitutional right to privacy, the government's need for tools to conduct investigations, and the interest of service providers in clarity and customer trust.

A primary reason that Congress adopted ECPA in 1986 was to provide sound footing for investment and innovation. In 1986, the fledgling wireless and Internet industries wanted to be able to assure potential customers that their communications were private. Congress recognized that consumers would not trust new technologies if the privacy of those using them was not protected. In the quarter century since the 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.
- **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 real-time, and is often stored in easily accessible logs files. Location data can reveal a person's movements, from which inferences can be drawn about activities and associations. Location data is augmented by very precise GPS data being installed in a growing number of 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.
- **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.

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, from the moment it is being typed to the moment it is opened by the recipient to the time it is stored with the email service provider. To take another example, a document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but the ECPA says that the same document stored with a service provider may not be subject to the warrant requirement.

- **Unclear standards:** ECPA does not clearly state the standard for governmental access to location information.
- **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." In the past 5 years, no fewer than 30 federal opinions have been published on government access to cell phone location information, reaching a variety of conclusions.
- **Constitutional uncertainty:** The courts are equally conflicted about the application of the Fourth Amendment to new services and information. A district court in Oregon recently opined that email is not covered by the constitutional protections, while the Ninth Circuit has held precisely the opposite. Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion.

This murky legal landscape does not serve the government, customers or service providers well. Customers are, at best, confused about the security of their data in response to an access request from law enforcement. 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 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.

Guiding Principles for ECPA Reform

The overarching goal of our review of the ECPA was 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.

We were guided by the following concepts:

- **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.

- **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, we focused on just a handful of the most important issues – those that are arising daily under the current 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.

Our principles do 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, we all agree that these principles provide a framework for opening a public dialogue on the issue.

Specific Background on ECPA Reform Principles

1. 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 the safeguards that the law has traditionally provided for the privacy of our phone calls or the physical files we store in our homes to private communications, documents and other private user content stored in or transmitted through the Internet "cloud"-- private emails, instant messages, text messages, word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks.

- 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.

2. 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.

- A warrant for mobile location information was first proposed in 1998 as part of the bipartisan Ashcroft-Leahy bill. It was approved 20 to 1 by the House Judiciary Committee in 2000.

3. 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 to a crime being investigated.

4. 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.

Members of Digital Due Process:

AOL
AT&T
Data Foundry
eBay
Google
Integra Telecom
Intel
Loopt
Microsoft
Qwest
Salesforce.com
TRUSTe

American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
Association of Research Libraries
Americans for Tax Reform
Bill of Rights Defense Committee
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Citizens Against Government Waste
Competitive Enterprise Institute
Computer & Communications Industry Association
The Constitution Project
Consumer Action
Distributed Computing Industry Association
Electronic Frontier Foundation
FreedomWorks
Information Technology and Innovation Foundation
NetCoalition
The Progress & Freedom Foundation

Individuals:

Patricia Bellia, Notre Dame Law School
David Berger, Wilson, Sonsini Goodrich & Rosati
Michael Carroll, American University, Washington School of Law
Fred Cate, Indiana University Law School
Danielle Keats Citron, University of Maryland School of Law
Ralph D. Clifford, University of Massachusetts School of Law
Susan Crawford, University of Michigan Law School
Susan Freiwald, University of San Francisco Law School

James Grimmelmann, New York Law School
Eric Goldman, Santa Clara University School of Law
Robert A. Heverly, Michigan State University College of Law
Dan Hunter, New York Law School and The Wharton School, University of Pennsylvania
Charles H. Kennedy, Wilkinson Barker Knauer, LLP
Liza Barry-Kessler, Privacy Counsel LLC
Mark A. Lemley, Stanford Law School
Jennifer Lynch, UC Berkeley Law School
Rebecca MacKinnon, Center for Information Technology Policy, Princeton University
Anthony Martin, Husch Blackwell Sanders LLP
Deirdre Mulligan, UC Berkeley iSchool
Paul Ohm, Professor of Law, University of Colorado
Scott Parsons, Portland State University
Frank A. Pasquale, Seton Hall Law School
David G. Post, Beasley School of Law, Temple University
Ira Rubinstein, New York University School of Law
Pam Samuelson, UC Berkeley Law School and iSchool
Katherine J. Strandburg, New York University School of Law
Jennifer Urban, UC Berkeley Law School
Michael Zimmer, School of Information Studies, University of Wisconsin-Milwaukee
Marc Zwillinger, Zwillinger Genetski LLP

For further information, contact:

James X. Dempsey
jdempsey@cdt.org
202-365-8026