Written Statement of the
Competitive Enterprise Institute, The Progress & Freedom Foundation,
Citizens Against Government Waste, Americans for Tax Reform, and
The Center for Financial Privacy and Human Rights

Before the
House Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties

September 23, 2010

Hearing on
ECPA Reform and the Revolution in Cloud Computing

Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Committee:

The undersigned public interest groups, think tanks, and advocacy organizations respectfully submit these comments to the United States House Committee on the Judiciary to urge Congress to amend U.S. laws to better safeguard citizens against unwarranted governmental access to private information held electronically by third parties. Such information includes emails, instant messages, and mobile locational data. We recognize the importance of ensuring that law enforcement agencies possess the tools necessary to effectively enforce the law and successfully prosecute criminals, but we also believe that the unnecessary vagueness and complexity of the current electronic privacy regime actually impede law enforcement efforts. We have joined the Digital Due Process Coalition (www.digitaldueprocess.org) to express our strong support for updating the Electronic Communications Privacy Act (ECPA). The Coalition has proposed that Congress establish clear, consistent, and technologically neutral rules governing the compelled disclosure by law enforcement of electronic information stored with service providers.

Obsolete Federal Privacy Laws Threaten the Emerging Cloud Computing Industry, Endangering Job Creation and Economic Growth at Home and Abroad.

To date, cloud computing[1] has transformed both global commerce and the daily lives of individuals worldwide for the better.[2] Cloud computing's rapid growth is expected to continue for the foreseeable future. Some experts believe that its ultimate impact on business, communications, and productivity will be nothing short of revolutionary.[3] Market research firm IDC estimates that cloud services will grow more than five times faster than traditional information technology products through 2014.[4] Growth in cloud-based services is also expected to fuel the creation of hundreds of thousands of jobs worldwide while also enabling significant productivity gains and economic growth.[5]

The success of cloud computing—and its benefits for the U.S. economy—depends largely on updating the outdated federal statutory regime that currently governs electronic communications privacy.

The privacy of sensitive information stored with cloud computing providers is a major concern for many consumers and business executives. According to a 2010 Harris Interactive poll, 81 percent of online Americans are concerned about the security of cloud computing services, while 62 percent say they would not entrust files containing personal information to cloud computing services.[6] A 2010 Zogby International poll found that 88 percent of Americans believe consumers "should enjoy similar legal privacy protections online as they have offline."[7] A 2009 survey commissioned by Microsoft found that 90 percent of senior business leaders and members of the public are "concerned about the security and private of personal data" in the cloud.[8] Federal government officials have reiterated these concerns. U.S. Chief Information Officer Vivek Kundra recently stated that government should "address various issues related to security, privacy, information management and procurement to expand cloud computing services."[9]

---

[1] According to NIST, "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

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

[3] *See* Jeffrey F. Rayport & Andrew Heyword, *Marketspace Point of View: Envisioning the Cloud: The Next Computing Paradigm*, March 20, 2009, pp. 2. http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.

[4] IDC, "Aid to Recovery: The Economic Impact of IT, Software, and the Microsoft Ecosystem on the Global Economy," October 2009 http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100623005419&newsLang=en .

[5] Frederico Etro, "The Economic Impact of Cloud Computing on Business Creation, Employment, and Output in Europe," Review of Business and Economics, 2009/2, pp. 179-208.

[6] David Linthicum, "Cloud security's PR problem shouldn't be shrugged off," *InfoWorld,* April 27, 2010. http://www.infoworld.com/d/cloud-computing/cloud-securitys-pr-problem-shouldnt-be-shrugged-776

[7] Zogby International, Results from June 4-7 Nationwide Poll (June 7, 2010) http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf.

[8] *See* Brad Smith at the Brookings Institution Policy Forum, "Cloud Computing for Business and Society," January 20, 2010, pp. 3. http://blog.seattlepi.com/microsoft/library/20100120smithspeech.pdf

[9] Vivek Kundra, White House Blog, "Streaming at 1:00: In the Cloud" (Sept. 15, 2009), available at http://www.whitehouse.gov/blog/streaming-at-100-in-the-cloud/

To be sure, storing information in the cloud entails numerous risks and vulnerabilities, many of which government is ill-suited to address.[10] Private firms are, after all, responsible for keeping sensitive user data safe from hackers and other cybersecurity threats.[11] But Congress and the courts are responsible for establishing reasonable safeguards to protect information stored in the cloud from unwarranted compelled disclosure to law enforcement. Unfortunately, the existing statutes governing this are woefully inadequate.

ECPA, the primary federal statute governing privacy in electronic communications, was enacted by Congress in 1986. While the law has been revised several times since then, many key sections remain largely unchanged.[12] In the 24 years since ECPA's initial enactment, technological evolution has profoundly altered how businesses and individuals communicate in ways that policymakers could not have envisioned in 1986. Service providers now house massive quantities of individuals' and businesses' sensitive information on their servers, thanks to the advent of now-ubiquitous communications platforms such as email, the World Wide Web, instant messaging services, blogs, social networks, and smartphones.[13]

Since 1986, computing power has doubled roughly every 18 months—in accordance with Moore's Law—and the cost of digital storage has plummeted.[14] This has enabled service providers to offer dramatically expanded—if not essentially unlimited—storage.[15] Cloud providers now offer a growing array of free, ad-supported data hosting services, such as Gmail, Mediafire, and Dropbox.[16] Such services have gained massive popularity among individual Internet users as well as small businesses.[17] Many large enterprises also use cloud computing services such as Microsoft's Azure, Salesforce CRM, and Amazon Simple Storage Service (S3).[18]

Today, hundreds of millions of individuals around the world take advantage of cloud computing services. Social networking site Facebook has more than 500 million active users, including about 150 million in the United States.[19] In other words, nearly *one out every two* Americans is currently an active Facebook user. Gmail, a leading webmail

---

[10] "Cloud Computing and Privacy," World Privacy Forum website, http://www.worldprivacyforum.org/cloudprivacy.html
[11] Clyde Wayne Crews, "Cybersecurity and Authentication: The Marketplace Role in Rethinking Anonymity—Before Regulators Intervene," *Knowledge, Technology & Policy*, Vol. 20 No. 2, pp. 97-105, http://www.springerlink.com/content/dq8522k3361757r4/
[12] *See* Justice Information Sharing Federal Statutes page. *Available at* http://www.it.ojp.gov/default.aspx?area=privacy&page=1285
[13] Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, at 4 (Feb. 23, 2009) http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf
[14] Clayton M. Christensen, *The Innovator's Dilemma*, 1997, Chapter One http://www.businessweek.com/chapter/christensen.htm
[15] Robert D. Atkinson & Andrew S. McKay, Information Technology & Innovation Foundation, *Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 14 (March 2007) http://www.itif.org/files/digital_prosperity.pdf
[16] *See e.g.* Susie Ochs, "Online Storage Battle: Which Cloud Back-Up Service Reigns Supreme?" *MacLife.com,* June 11, 2009. http://www.maclife.com/article/reviews/online_storage_battle_which_cloud_backup_service_reigns_supreme
[17] Robert Cheng, "'Cloud Computing': What Exactly Is It, Anyway?," *The Wall Street Journal,* February 8, 2010. http://online.wsj.com/article/SB10001424052748703580904574638391318085158.html
[18] Charlton Barreto, "Cloud Computing: Rich Services Cloud: The Value Proposition," Intel Technology Strategy, November 2009, pp. 23. http://charltonb.typepad.com/talks/110209-cbb-cloud/Cloud%20Computing%20-%20Rich%20Services.pdf
[19] *See* Facebook Press Room Statistics. *Available at* http://www.facebook.com/press/info.php?statistics

service, has more than 175 million active users.[20] As the use of cloud services grows, popular awareness of the attendant privacy risks grows alongside it. As a result, individuals and businesses are increasingly demanding robust information security assurances from cloud providers—and cloud providers are responding by competing on privacy and security.[21] But they can do little to assure users that their data will remain free from unwarranted governmental access.

In many cases, ECPA authorizes law enforcement to compel service providers to disclose potentially sensitive information without first obtaining a search warrant based upon probable cause or without any judicial authorization at all.[22] For instance, a law enforcement official who wishes obtain the contents of a communication in "electronic storage" for more than 180 days may be able to compel a provider to disclose the communication through a mere subpoena, which is typically issued with no judicial scrutiny.[23]

In recent months, there has been growing mainstream media attention on the ease with which government can access user information stored with remote service providers.[24] For instance, *PC World*'s 2010 article, "Why ECPA Should Make You Think Twice about the Cloud," discussed in great detail the privacy risks of storing data with cloud providers.[25] Google recently launched a tool disclosing the number of requests for user data it received from U.S. law enforcement in the second half of 2009 (the figure was 3,580).[26] In the first half of 2010, the number of requests Google received rose to 4,287—an increase of 20 percent compared to the previous six-month period.[27] A June 2010 *Wall Street Journal* article chronicled the recent rise of venture capital-backed privacy startups, noting that, "[I]n the wake of recent privacy flaps involving AT&T, Facebook, Apple Inc. and others, consumer awareness has grown."[28] Prompt action by Congress to strengthen federal laws safeguarding the privacy of information stored in the cloud is growing more important by the day as Americans become ever more reliant on cloud computing in all aspects of life.[29]

---

[20] Jessica E. Vascellaro, "Gmail, Too, Seeks to Rival Facebook," *The Wall Street Journal,* February 8, 2010. http://online.wsj.com/article/SB10001424052748703630404575053480962942848.html

[21] David Navetta, "Cloud Providers Competing on Data Security & Privacy Contract Terms," InfoLawGroup.com, April 12, 2010. http://www.infolawgroup.com/2010/04/articles/cloud-computing-1/cloud-providers-competing-on-data-security-privacy-contract-terms/

[22] *See* 18 U.S.C. § 2703(b)(1)(B), http://www.law.cornell.edu/uscode/18/usc_sec_18_00002703----000-.html

[23] *See* U.S. Department of Justice Electronic Surveillance Manual at 25. *Available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf

[24] *See e.g.* Google News search for "Electronic Communications Privacy Act," which lists 320 news articles for 2010. http://www.google.com/search?q=%22Electronic+Communications+Privacy+Act+%28%22&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a#q=%22Electronic+Communications+Privacy+Act%22&hl=en&client=firefox-a&rls=org.mozilla:en-US:official&tbs=nws:1,cd_min:2010,cd_max:2010,cdr:1&source=lnt&fp=180bd06780889f90

[25] Tony Bradley, "Why ECPA Should Make You Think Twice about the Cloud," *PC World*, March 30, 2010. http://www.pcworld.com/businesscenter/article/192989/why_ecpa_should_make_you_think_twice_about_the_cloud.html

[26] *See* Google Transparency Report FAQ *Available at* http://www.google.com/governmentrequests/overview.html

[27] Ryan Singel, "Feds' Requests for Google Data Rise 20 Percent,' *Wired Threat Level,* September 21, 2010. http://www.wired.com/threatlevel/2010/09/google-government-requests-rise

[28] Pui-Wing Tam and Ben Worthen, "Funds Invest in Privacy Start-Ups," *The Wall Street Journal,*" June 20, 2010. "http://online.wsj.com/article/SB10001424052748703438604575315182025721578.html

[29] Lisa Banks, "Cloud computing to increase annual data growth 24-fold by 2020: study," *CIO,* May 5, 2010. http://www.cio.com.au/article/345435/cloud_computing_increase_annual_data_growth_24-fold_by_2020_study/

If Congress fails to reform privacy laws, some Americans will choose not to take advantage of cloud computing, while others will simply turn to data encryption solutions for protecting their data. Such solutions could distort the evolution of cloud computing in harmful ways. Several services today allow users to store encrypted information in the cloud without sharing the key with the provider.[30] While this arrangement is ideal in many circumstances—encryption maximizes data security and minimizes the risks of unwarranted governmental intrusion—it also comes at a cost.

First, users will bear the direct cost of paying for encrypted services, which are often slower than unencrypted services (a significant cost, since some cloud computing applications already start from a performance disadvantage compared to desktop-based applications).[31] Second, if cloud service providers cannot access in plaintext the information stored by their users, they may not be able to rely on advertising to support those services. The most popular cloud service in use today is webmail, and Google's Gmail service demonstrates how targeted advertising (ads based on algorithmic scanning of keywords in an email) can support *dramatic* improvements in the quality of a service. When Gmail launched in 2004, Yahoo! Mail (then, as now, the leading webmail provider) offered customers less than 10 megabytes of email storage, yet Gmail offered an astounding 1 gigabyte of storage.[32] Today that figure is over 7.5 GB, and Gmail has become much more than a plain vanilla email service, supporting a variety of applications and features unimagined in 2004.[33] But Gmail's ad-serving feature simply would not work if users routinely encrypted their messages and held onto the encryption key. Some users *might* pay for such innovative services, but on the whole, there would likely be less funding available for Gmail and similar cloud services. Consumers would pay more or get less—on top of the cost of encryption itself. In many ways, therefore, ECPA's failure to protect our digital communications and documents amounts to a "tax" on Americans.

The Digital Due Process Coalition's Proposed Reforms to the Electronic Communications Privacy Act Will Preserve the Building Blocks of Law Enforcement Investigations.

The reforms urged by the Digital Due Process coalition will not substantially constrain legitimate law enforcement investigations or other governmental efforts to safeguard U.S. national security and combat terrorism. Our proposed reforms do not alter the Foreign Intelligence Surveillance Act, the statute used to monitor terrorists and spies and to gather foreign intelligence to prevent terrorist attacks. Although our proposed reforms would impose some additional limitations on the ability of law enforcement to compel service

---

[30] *See e.g.* Mozy Privacy Commitment, "Choose Mozy's encryption key using 448-bit Blowfish or manage your own key using military-grade 256-bit AES to secure your data during storage." http://mozy.com/privacy/commitment/

[31] R. Colin Johnson, "IBM Encryption Breakthrough Could Secure Cloud Computing," *Smarter Technology,* October 14, 2009. http://www.smartertechnology.com/c/a/Technology-For-Change/IBM-Encryption-Breakthrough-Could-Secure-Cloud-Computing/

[32] *See* Chris Anderson, Free: The Future of a Radical Price at 112-118 (2009)

[33] *See* Digital Prosperity *supra* Note 15, at 8 (The falling cost of storage is "why Web companies like Google, Yahoo, and Microsoft are providing consumers with large amounts of free Web-based storage for their email, photos, and other files…But because memory is now so cheap, Google and other companies can afford to give vast amounts of it away for free, paying for it through unobtrusive advertisements.").

providers to disclose user information in the criminal context, the proposed limitations are consistent with the spirit of the Fourth Amendment to the United States Constitution. Our nation's founders rightly recognized the importance of balancing the need to effectively enforce the laws of the land against the right of citizens to be free from unwarranted governmental intrusion into their private affairs.[34] Therefore, they sought to protect Americans against unreasonable search and seizure by government through the requirement that law enforcement agents first obtain a warrant from a judge upon a showing of probable cause.[35]

U.S. communications privacy laws no longer strike an acceptable balance between the two important priorities of privacy and security. In effect, they fail to protect the "papers and effects" of the Digital Era. Congress never voted for less privacy. Rather, consumers changed the way they communicate as technology evolved, and the law simply has not kept up with those changes. The resulting deficiencies pose a grave threat to the individual freedoms enshrined in the Constitution. Alex Kozinski, Chief Judge of the U.S. Court of Appeals for the Ninth Circuit and a Reagan appointee, observed in a recent dissent in a case involving GPS tracking that, "The needs of law enforcement … are quickly making personal privacy a distant memory. 1984 may have come a bit later than predicted, but it's here at last."[36]

ECPA and other federal wiretap statutes currently contain a number of special exceptions for child pornography, life-threatening emergencies, kidnapping, and other exigent and serious circumstances.[37] The Digital Due Process coalition is not urging Congress to amend these provisions.[38] Rather, the Coalition's principles for reform would leave existing exceptions untouched, and preserve the building blocks of law enforcement investigations – subpoenas, court orders based on lower standards of proof, and warrants when there is probable cause.

Orin Kerr, a Professor at George Washington University School of Law who formerly served as a computer crimes prosecutor for the Justice Department and as an assistant U.S. attorney for the Eastern District of Virginia, recently testified before the U.S. House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties that, "[R]eforms [to ECPA] are surely needed."[39] While emphasizing the importance of maintaining a "balanced approach to the new investigations involving new network technologies that the Fourth Amendment strikes in the physical world," Kerr also expressed support for three of the four proposals advocated by the Digital Due Process coalition. In a 2004 *George Washington Law Review* article, Kerr stated that, "[T]he most

---

[34] Orin Kerr, "Applying The Fourth Amendment To The Internet: A General Approach," *Stanford Law Review,* Vol. 62, Issue 4, pp. 1017. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860

[35] *Ibid,* pp. 1044.

[36] *See* dissent by Chief Judge Kozinski in *United States v. Pineda-Moreno,* U.S. No. 08-30385, August 12, 2010, pp. 11504. http://www.ca9.uscourts.gov/datastore/opinions/2010/08/12/08-30385.pdf

[37] *See e.g.* Electronic Communications Privacy Act Rule by Exceptions, Cybertelecom.org, *available at* http://www.cybertelecom.org/security/ecpaexception.htm

[38] J. Beckwith Burr, "The Electronic Communications Privacy Act of 1986: Principles for Reform," WilmerHale, pp. 4. http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf

[39] *See* Orin Kerr, "Testimony of Orin S. Kerr before the United States House of Representatives Committee on the Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties Hearing on Electronic Communications Privacy Act Reform," May 5, 2010. http://volokh.com/wp/wp-content/uploads/2010/05/KerrTestimony.pdf

obvious problem with the current version of the SCA is the surprisingly weak protection the statute affords to compelled contents of communications under the traditional understanding of ECS and RCS" (Electronic Communications Services and Remote Computing Services). He recommended that Congress "bolster the privacy protections that cover stored content held by an RCS or by an ECS for more than 180 days in 18 U.S.C. § 2703(b)."[40]

Conclusion

If Congress wishes to ensure Americans enjoy the full benefits of the cloud computing revolution, it should simply reform ECPA in accordance with the principles proposed by the Digital Due Process coalition, rather than enacting distortionary new subsidies or industrial policies. Requiring that law enforcement obtain a search warrant from a judge upon a showing of probable cause before rifling through the contents of our electronic communications and digital documents should be uncontroversial. Such a requirement would extend the protections of the Fourth Amendment to our digital "papers and effects," and would *not* interfere with law enforcement or national security investigations. We, the undersigned nonprofit organizations dedicated to the principles of limited government and individual rights, ask Members of both parties to lend your support to these proposed reforms.

Respectfully Submitted,

Ryan Radia
Associate Director of Technology Studies
Competitive Enterprise Institute

Berin Szoka
Senior Fellow and Director, Center for Internet Freedom
The Progress & Freedom Foundation

Thomas A. Schatz
President
Citizens Against Government Waste

Kelly William Cobb
Executive Director, Digital Liberty Project
Americans for Tax Reform

J. Bradley Jansen
Director
Center for Financial Privacy and Human Rights

[40] Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," *George Washington Law Review,* Vol. 72, 2004, pp. 30-31. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860