Before the
Department of Commerce
Washington, DC

In re	:	
Information Privacy and Innovation in the Internet Economy	:	Docket No. 100402174-0175-01

COMMENTS OF
COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

The Computer and Communications Industry Association ("CCIA") respectfully submits these comments in response to the U.S. Department of Commerce ("DOC"), National Telecommunications and Information Administration's ("NTIA"), Notice of Inquiry in the matter of Information Privacy and Innovation in the Internet Economy.[1] Although the DOC raises numerous important issues, CCIA does not seek to address them all. Instead, these comments address: (1) revising the Electronic Communications Privacy Act[2] ("ECPA") in order to create a clear set of working standards for both individuals and businesses; (2) distinguishing between tracking by applications and websites and tracking by network operators offering Internet access, and the potentially harmful effects of the use of deep-packet inspection ("DPI") by internet access providers ("IAPs") for uninvited intrusions at the network level; (3) ensuring that privacy policy adequately addresses the continuing advancement in technologies, including the rise of remote computing services ("cloud computing") which may recognize no geographical boundary, and the widespread availability of geolocation data.

1 "Information Privacy and Innovation in the Internet Economy; Notice of Inquiry," 75 Fed. Reg. 78 (April 2010), pp. 21226-21231.
2 The Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510, *et seq.*

CCIA is a non-profit international trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. CCIA members employ nearly one million people and generate annual revenues exceeding $250 billion.[3]

I. Introduction

The U.S. possesses a unique opportunity to lead the world in safeguarding civil liberties, but in order to display sufficient credibility to do so, our own privacy policy must do more than merely mitigate perceived intrusions. Instead, the U.S. should adopt policies that broadly protect Internet users' free speech and privacy rights from overreaching law enforcement as digital information moves into contexts different from those in which traditional privacy protections were formed. Inquiries into the current state of privacy policy should go beyond examining potential online commercial abuses to look at hidden telecommunications network surveillance and undue government intrusions.

CCIA commends the DOC for taking another step in that direction by raising the increasingly important issue of privacy in initiating its Information Privacy and Innovation in the Internet Economy proceeding. CCIA urges the DOC to cooperate with other interested bodies, including the U.S. Department of Justice ("DOJ"), the U.S. Office of Science and Technology Policy ("OSTP"), the Federal Trade Commission ("FTC"), the Federal Communications Commission ("FCC"), and other foreign governments in reviewing the current state of U.S. privacy law and policy.

[3] A complete list of CCIA's members is available online at http://www.ccianet.org/members.

Concerns over privacy continue to rise as innovation and technological developments advance at a rapid pace. The Internet's expansion brings consumers new and exciting ways to communicate and engage with one another, the government, potential employers, and society as a whole. However, in doing so, more and more consumers are sharing sensitive and personal information, data, and communications online. U.S. privacy policy should be crafted in a way that allows businesses and consumers to understand the ramifications of this shift to sharing more private information online.

Even when no actual privacy loss occurs, the mere perception of privacy loss in personal and/or business matters can spur widespread damage in consumer confidence. When data security is lacking, business users also lose confidence in online transactions. In March 2010 the FCC released its National Broadband Plan ("NBP") calling for nearly ubiquitous access to broadband.[4] If consumers fear that their private information is at risk, adoption of broadband will be slowed, thus hindering the goals set forth by the FCC's NBP.

II. Revision of ECPA will help clear the air of uncertainty surrounding privacy laws and allow individuals and businesses to better understand their privacy rights and how to comply with and invoke the protection of U.S. privacy laws.

Technologies are not immune from governmental overreaching and any review of U.S. privacy policy must take into account governmental intrusions. As a general proposition, CCIA supports the application of basic Forth Amendment protections against undue search and seizure to electronic communications. CCIA also supports the ECPA revisions advanced by the Digital Due Process Coalition ("DDP"), of which CCIA is a member.

[4] Omnibus Broadband Initiative, Federal Communications Commission, Connecting America: The National Broadband Plan (2010).

A. As it stands, Courts treat harshly the concept of Fourth Amendment protections in the Internet realm.

Historically, the Fourth Amendment protected postal mail from governmental inspection during delivery. This privacy right in one's mail extended to mail carried by the U.S. Postal Service ("USPS"), as well as private carriers such as United Parcel Service and Federal Express. While some minimal exceptions applied,[5] people generally held privacy rights in mail sent by or delivered to them. As e-mail becomes the more dominant form of communicating, U.S. courts have been hostile to the idea of extending these postal mail Fourth Amendment protections to electronic communications.

A recent decision by the U.S. District Court for the District of Oregon highlights the potential troublesome outcome for Fourth Amendment protection in the context of ECPA. In *In re Application of U.S. for Search Warrant*, the District Court concluded that law enforcement officials did not have to inform an e-mail account holder of a warrant to search the contents of his or her e-mail account.[6] Instead, the court found sufficient notice served only to the IAP and not the account holder. The court premised its decision on the theory that a person must access the Internet through an IAP and, in doing so, the user's information passes through, or may even be stored on, servers owned by the IAP. By means of this process, the Court concluded that the information was no longer private information contained in the home and, thus, not protected by ECPA.

Similarly, the Eleventh Circuit recently rejected extension of Fourth Amendment protection to e-mails. In *Rehberg v. Paulk*, the Eleventh Circuit held that, "a person…loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a

---

[5] No privacy right extended to USPS mail sent as "fourth class," which reserved for the USPS the right to inspect the mail. Further, the protection applied only to the *content* of the mailing, not to anything on the outside of the envelope or the package (i.e. addresses and names).

[6] *In re Application of U.S. for Search Warrant*, ___ F.Supp.2d ___, 2009 WL 3416240 (D. Or. 2009)

third party."[7] The Court found the government's subpoenaing of defendant's e-mails from an IAP to not violate the defendant's Fourth Amendment rights as the e-mails were subpoenaed directly from the IAP and not, "an illegal [search of defendant's] home computer for e-mails."[8]

The courts' unwillingness to extend Fourth Amendment protections to electronic communications, in a world where e-mail serves as a dominant form of communication, will continue to shake consumer confidence in adoption of broadband as an efficient tool for daily communications. Protection from governmental intrusion must evolve as technology evolves. In order for the pervasiveness of e-mail to continue, it is vital that consumers can expect to receive the same protection for an e-mail that they receive in a handwritten letter. E-mail users have established an expectation of privacy in their communications and, as e-mail becomes more and more commonly used, this expectation will only deepen.

Since the Fourth Amendment should extend to anywhere "a reasonable expectation of privacy" exists,[9] the protections prescribed by the Fourth Amendment should be extended to electronic communications in order to preserve consumer confidence. At least two courts have recognized this and found, unlike the Eleventh Circuit's later *Rehberg* decision, that e-mails stored in a web-based e-mail account[10] and text messages stored with a service provider[11] to be protected by the Fourth Amendment. These decisions better develop U.S. privacy policy in accordance with technological advancements.

---

7 *Rehberg v. Paulk*, ___ F.3d ___, 2010 WL 816832 (11th Cir. Mar. 11, 2010).
8 *Id.*
9 *Katz v. U.S.*, 389 U.S. 347, 361 (1967).
10 *Warshak v. U.S.*, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc on other grounds*, 532 F.3d 521 (6th Cir. 2008).
11 *Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008), *cert. granted sub nom. City of Ontario v. Quon*, 78 U.S.L.W. 3395 (U.S. Dec. 14, 2009) (No. 08-1332).

B. DDP's proposed ECPA revisions help clarify privacy standards for both individuals and businesses and effectively accommodate technological advancements, including the tracking and collection of geolocational data.

DDP advocates four specific ECPA revisions that seek better protection for data shared or stored online.[12] These revisions will also allow for better protection from governmental bulk data requests. CCIA agrees with DDP's assessment that such revisions are necessary to better ensure clarity for both individuals and businesses in what ECPA standards apply to information and data online.

The first recommended ECPA revision would require law enforcement to obtain a search warrant based on probable cause before obtaining private communications or documents stored remotely.[13] Such a revision merely extends the traditional privacy protections provided to documents physically held in the home to the Internet realm. The second revision would require law enforcement to obtain a search warrant before tracking people's location via cell phones or other devices.[14] The third revision would require law enforcement to submit proof that the information sought is relevant to a criminal investigation before electronic surveillance begins.[15] The fourth revision would require law enforcement to submit proof the information sought is not only relevant to a criminal investigation, but is in fact needed, before it may obtain bulk information about broad categories of unknown telephone or internet users.[16]

Additionally, DDP's proposed ECPA revisions would help companies and individuals better understand the privacy concerns of an increasingly important technological development:

---

[12] "Specific Background on ECPA Reform Principles," Digital Due Process Coalition, available online at http://www.digitalddueprocess.org/index.cfm?objectid= C00D74C0-3C03-11DF-84C7000C296BA163.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

the tracking and collection of geolocational data. Mobile phone service providers are being bombarded with law enforcement requests for both real-time tracking of mobile devices and collected geolocational data of mobile devices in connection with searches and surveillance. Meanwhile, privacy advocates' argue that disclosure of such information violates the subscriber's privacy. Geolocational data may also be collected by social networking websites based on the user's location, often through a global positioning system ("GPS") on the user's mobile device or triangulating the device's signal via cell towers. DDP's proposed ECPA revisions help solidify standards of when telecommunications companies can and cannot hand over users' geolocational data to law enforcement authorities.

Revision of ECPA would help tech companies better draft policies that strike a balance between operational needs and user privacy and security. As it stands now, certain law enforcement legislation requires tech companies to keep large databases of retained consumer information. These requirements not only place onerous burdens on the tech companies themselves, but also result in a weakened consumer trust in both the companies and Internet technology itself. Although companies are trying to draft such balanced data retention policies right now, the current state of ECPA results in companies being stuck between privacy advocates demanding less retention and law enforcement favoring increased retention, with ECPA providing little-to-no clarity on how to proceed.

III. U.S. privacy policy should recognize a distinction between tracking by websites and Internet services at the application level and intrusions by IAPs at the network level, and prohibit any use of DPI by IAPs to track user activity, gather user information, inspect the content of user's messages, or for any other illegitimate purpose.

The differing level of user choice calls for a distinction between technologies used at the application level and technologies used at the network level. At the application level, consumers

may not only have the ability to control what information is collected about them, but also have a better ability to respond to any inappropriate behavior by the service provider. These options often do not exist at the network level.

Users have a greater amount of control at the application level as a result of competition among service providers. Multiple companies often offer the same or a similar product allowing a user of one application to leave that service provider without penalty or inconvenience, if and when it acts inappropriately, and fairly easily migrate to another application offering the same or similar services. As a result, companies acting at the application level know they must implement and act according to pro-consumer policies, or risk losing customers to a competitor.

Users generally do not have the same ability to control and respond to IAP behavior at the network level because the network operators/IAPs lack the competition found at the application level. The high barriers to entry into the Internet access business leads to fewer companies within a given area providing service choice for consumers. Thus, fewer choices leave consumers unable to switch from one IAP to another service.

Additionally, IAPs often engage in practices that make departure from their service even more difficult. For instance, IAPs will often offer a significantly lower monthly rate when the consumer signs a contract agreeing to utilize that IAP's services for some period of time, sometimes upwards of two years. This results in more consumers binding themselves to that IAP for an extended period of time in order to receive the lower, more affordable, rate. Further, IAPs often provide other telecommunications services, such as cable television and/or telephone. Those multi-faceted companies will often bundle their Internet access service with the other television and/or telephone services, further locking in the consumer.

The consumer's lack of control at the network level is of even greater concern because the use of DPI technology at the network level allows IAPs access to a great amount of consumer personal data and a greater ability to engage in end-user tracking of all activity online. Such access and the potential for illegitimate uses highlights why the use of DPI by IAPs at the network level should be prohibited where the IAP fails to give full disclosure to the consumer of its DPI activity and/or the IAP fails to receive express consent to engage in such DPI activity from the user.

The disclosure and consent requirements for use of DPI should be subject to certain standards. Informing the consumer should require the IAP's disclosure to the consumer of:

(1) The purpose of the inspection;

(2) What will be inspected and how it will be inspected;

(3) All uses that will be made of the information gleaned from the monitoring; and

(4) The fact that consent means waiver of all privacy rights, other civil privileges and confidentiality protections.

In explaining any claimed waiver of rights, the IAP should ensure that customers completely understand when their terms of service claim to forfeit any legal privilege, including attorney-client, priest-penitent, doctor-patient, or trade secret privileges. Further, any such term of service is problematic and should be subjected to federal review. Lastly, IAPs should not be permitted to make consent to DPI a mandatory term of the service contract.

CCIA recognizes that DPI may prove valuable in an IAP's attempts to control network integrity and security. As such, DPI should be permitted for those limited purposes only. Any illegitimate use of DPI by IAPs, including the gathering of user-specific information and end-user tracking, should be prohibited without disclosure to the user and the user's express consent.

IV. An updated U.S. privacy policy should address where privacy stands in continually advancing technologies which may recognize no geographical boundary, such as cloud computing.

Uncertainty abounds for both consumers and businesses in understanding what privacy standards apply to new online applications and cloud computing due to the patchwork nature of current federal laws. Further complicating matters, new technologies such as cloud computing may recognize no geographical boundary. The current sector-specific laws result in consumers having more protection in one area than in another, making consumers unsure what level of protection will apply where. Instead, both businesses and consumers need a modernized and clear set of baseline rules taking into account these continually advancing technologies that necessarily have a multijurisdictional existence.

A. The rise in popularity of cloud computing requires clarification of what privacy standards will apply to information held in the cloud.

Cloud computing becomes more and more widely used as IAPs provide faster Internet speeds and data storage fees drop.[17] A 2008 Pew Internet study reports that approximately 40% of U.S. Internet customers have engaged in cloud computing, with approximately 59% of those people being between the ages of 18 and 29.[18] While cloud computing offers invaluable tools for cooperation and co-creation, the storage of documents and files on third party servers raises critical privacy questions.

---

[17] "Cloud Computing: Storm Warning for Privacy?," at 1, ACLU of Northern California ("ACLU Report"), available online at http://www.dotrights.org/cloud-computing-storm-warning-privacy-issue-paper (last accessed on June 1, 2010).

[18] "Use of Cloud Computing Applications and Services," Pew Internet and American Life Project ("Pew Report"), available online at http://www.pewinternet.org/Reports/2008/ Use-of-Cloud-Computing-Applications-and-Services.aspx?r=1 (Sep. 2008) (last accessed on June 1, 2010).

i. Applicability of Fourth Amendment protections to cloud computing requires clarification.

Currently, both the businesses that hold consumer data and the individuals whose data is held face uncertainty in whether the Fourth Amendment protections against unreasonable search and seizure apply to the cloud. The *Katz* case extended Fourth Amendment protections to any "reasonable expectation of privacy,"[19] and a subsequent line of cases extended the protections to items such as personal containers (even if left with another person or in a common area)[20], safety deposit boxes,[21] rented storage lockers,[22] personal computers (even if completely under the control of another),[23] and files on networked computers.[24] Meanwhile, the "business record exception," created by the Supreme Court before the Internet age, says no reasonable expectation of privacy can be had when a person turns over information to a third-party business.[25]

In order for certainty to prevail, this conflict must be resolved. Fourth Amendment protections should be extended to cloud computing in order to match consumer expectations, the promotion of innovation, and the continued prevalence of the Internet. Doing so will not only prompt further adoption of such valuable technologies and spur business development, but will also promote further innovation on the Internet as a whole.

---

[19] *Katz*, 389 U.S. at 361 (1967).

[20] *See* ACLU Report, at 5, *citing U.S. v. Most*, 876 F.2d 191 (D.C. Cir. 1989) (finding a plastic bag inadvertently left with a grocery clerk protectable) and *U.S. v. Block*, 590 F.2d 535 (4th Cir. 1978) (finding a locked footlocker in a common area to be protected).

[21] *See* ACLU Report, at 5, *citing U.S. v. Spilotro*, 800 F.2d 959 (9th Cir. 1985).

[22] *See* ACLU Report, at 5, *citing U.S. v. Karo*, 468 U.S. 705(1984).

[23] *See* ACLU Report, at 5, *citing U.S. v. Barth*, 26 F.Supp.2d 929 (W.D. Tex. 1998).

[24] Protection may not attach if "there is a clear policy of monitoring network use." *See* ACLU Report, at 5, *citing U.S. v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007) and *U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000).

[25] *See* ACLU Report, at 6, *citing U.S. v. Miller*, 425 U.S. 435 (1976) (finding banking records not protectable) and *Smith v. Maryland*, 442 U.S. 735 (1979) (finding phone records of numbers dialed unprotectable).

ii. The current federal statutory regime creates a climate of uncertainty around cloud computing and must be modernized to accommodate cloud computing.

Current federal privacy statutes require updating in order to address cloud computing. For instance, cloud computing post-dates ECPA and, thus, unsurprisingly is not defined by it. Updating laws to extend privacy coverage to cloud computing services will not only preserve consumer privacy but also encourage loyalty and trust in new beneficial technologies like cloud computing.

In addition to DDP's proposed ECPA revisions discussed above, Microsoft proposed privacy legislation directly addressing cloud computing in January 2010.[26] The proposed legislation followed a Microsoft-sponsored survey reflecting a significant excitement surrounding cloud computing.[27] However, that same study showed that 90 percent of those excited about cloud computing are also concerned about data security within the cloud.[28]

Microsoft's proposed legislation seeks four things:[29]

(1) "Improve[d]…privacy protection and data access rules to ensure users' privacy," specifically calling for revision of ECPA to "clearly define and provide stronger protections for consumers and businesses;"

(2) "Modernization of the Computer Fraud and Abuse Act" giving law enforcement the tools necessary to go after hackers and prevent online crime;

(3) Establishing "truth-in-cloud-computing principles" so that businesses and individuals will know how their data is accessed and used and how their data will be protected online; and

---

[26] *See* "Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud," Microsoft press release, Jan. 20, 2010, available online at http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx (last accessed on June 1, 2010).

[27] *See Id.* (reporting, "58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing…").

[28] *See Id.*

[29] *Id.*

(4) Creation of a multilateral agreement addressing data access issues across national borders.

Implementation of these four measures will help businesses and individuals to better understand privacy concerns in the cloud. With more certainty will come more investment and innovation in this new and exciting technology. In fact, an adequate update of the current legislative framework to accommodate technological advancements could spur investment and innovation in not just cloud computing, but across the Internet as a whole.

V. Conclusion

Modernizing the current state of U.S. privacy policy would go a long way toward promotion of innovation and investment across the Internet. With the current veil of uncertainty surrounding privacy online, individuals and businesses may have reservations about fully embracing all the possibilities the Internet has to offer.

Respectfully Submitted,

/s/ Ed Black
Ed Black, President & CEO
Catherine Sloan, Vice President Government Relations
Gregory Egan, Law Clerk
Computer & Communications Industry Association
900 Seventeenth Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070