Statement of

The Computer & Communications Industry Association (CCIA)

Before the

Committee on the Judiciary
U.S. Senate

"The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age"

September 22, 2010

As a non-profit association active in policy debates for over 35 years and whose membership includes companies from all parts of the telecommunications and information technology ecosystem, the Computer & Communications Industry Association ("CCIA") cares deeply about both the economic and civil liberties consequences of privacy regulations and laws. CCIA has been concerned with privacy since its founding and has been a vocal advocate in recent years against overreaching government surveillance. Ensuring the privacy of users and consequently earning their trust is essential for our industry to flourish. However, we also recognize that poorly worded regulations or outdated laws can have disastrous consequences not just for user privacy, but for legitimate, cutting-edge business practices as well.

In today's Internet age, application of the Electronic Communications Privacy Act[1] ("ECPA") to real life situations proves increasingly problematic. Specifically, the information technology and telecommunications industries face two major areas of difficulty and uncertainty in the context of ECPA compliance: (1) the treatment of geolocational information about individuals; and (2) the levels of protection for data in a cloud computing environment. Social networking is yet another alternative platform for private personal communications not addressed by ECPA. Application of ECPA to such new and increasingly prevalent technologies is far from clear. However, these difficulties are of no surprise. The unique challenges and difficulties surrounding these new technologies could not have been foreseen in 1986 when ECPA was enacted. These new and exciting technologies represent leaps in

[1] 18 U.S.C. 2510, *et seq.*

innovation and business practices from what Congress was looking at over 25 years ago when it drafted ECPA. As such, ECPA urgently needs a significant update to bring it into harmony with the early 21st century realities of digital electronic commerce and communications.

Service providers need solidified standards on how to handle consumer information and data, especially in the cases of geolocational information and cloud computing. Currently, providers are left with little to no guidance in how to balance operational needs, governmental requirements, and consumers' privacy and security. For instance, certain law enforcement legislation currently requires service providers to maintain large databases of retained consumer information. These requirements not only place extraordinary burdens on the provider companies themselves, but also weaken consumer trust in both the companies and the Internet as a whole. Microsoft Associate General Counsel Michael Hintze recently noted that ECPA has made it difficult for Microsoft to, "market itself as protecting users' privacy."[2] Companies across the information technology and telecommunications industries face the same or similar difficulties.

Mobile devices have fundamentally changed the way we communicate and provide a new way of tracking an individual's location, movements, and patterns of activity. Today, cell phones and mobile broadband devices generate a steady stream of location data necessary both for basic network operations and for innovative location-based services. This location data can be intercepted in real-time and

[2] Louis Trager, "Civil Libertarians Wish CDT-Led Coalition Would Go Further on Changing ECPA," Warren's Washington Internet Daily, Vol. 11, No. 165 (August 26, 2010).

stored in logs. Service providers in the telecommunications and information technology industries need a clear standard governing the terms under which they must hand over subscribers' geolocational data to law enforcement authorities. Currently, ECPA lacks such a standard. The sensitivity of geolocational data makes certainty and clarity in its handling that much more important. The collection of an individual's real-time locational data reflecting that person's current exact location is much more intrusive than the collection of past data such as a receipt indicating that person bought a venti latte from a certain Starbucks location this morning. Further, and potentially even more troubling considering the sensitivity of the information, consumers do not always know what kind of information is being collected about them and sometimes don't even know that any information is being collected at all. With more people using smartphones,[3] many of which contain global positioning systems ("GPS") that allow for nearly exact tracking,[4] a growing number of consumers are likely to have their locational information tracked and collected without being aware of it.

---

[3] The percentage of U.S. consumers owning smartphones has risen from 21% in October 2007 to 32% in December 2008 and 42% in December 2009. Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services, WT Docket No. 09-66, *Fourteenth Report*, FCC 10-81 at 92 (rel. May 20, 2010). Additionally, CTIA's "Mid-Year 2009 Wireless Indices Report" indicates that 40.7 million smartphones were in service as of June 30, 2009. *Id.*

[4] While GPS is not the only way of tracking and collecting subscribers' locational information, it can provide a more exact and precise location than tracking through triangulation. Providers can track and collect locational information through triangulation by pinging a mobile device with a signal sent from multiple service towers in order to determine where between those towers the device is located.

Cloud computing is another relatively recent technological development that creates widespread legal and business uncertainty regarding compliance with ECPA. Cloud computing utilizes the Internet's high-speed transportation paths to allow users to create, edit, and store data remotely on servers located elsewhere in the world rather than on one's own computer resources. Ten years ago, let alone twenty five years ago when ECPA was enacted, cloud computing was inhibited by slow data transmission and high storage costs. However, since that time data transmission speeds have increased exponentially and the price of data storage has dropped significantly. Data transmission speeds have now increased to the degree of allowing enterprise users nearly instantaneous access to remotely stored data, thus making cloud computing a viable option in the business world. Similarly, cheaper storage costs and search functionality have facilitated the saving and accessing of many years' worth of e-mail messages. Consumers do not necessarily have a lower expectation of privacy with respect to older e-mails as opposed to more recent messages. Thus, the continually increasing speed of data transmission coupled with a decreasing price for storage has created a setting where cloud computing now provides an attractive and affordable alternative for business users to augment or replace costly on-site computer resources. This is especially key for new and small businesses where the start-up costs of purchasing and maintaining on-site computer resources could be prohibitive.

Information technology and telecommunications companies have responded to the increased interest of consumers and enterprise users by developing and offering a wide array of cloud computing services which can be broken down into

three categories: (1) Software-as-a-Service ("SaaS"); (2) Platform-as-a-Service ("PaaS"); and (3) Infrastructure-as-a-Service ("IaaS"). Recent years have seen a proliferation of free or very low cost SaaS services such as e-mail (i.e. G-mail and Hotmail) and personal financial (i.e. mint.com) software that utilize cloud resources to lower prices and the Internet's reach to enhance functionality. E-mail services today provide millions of consumer and business users a nearly limitless storage and access from any computer, all for free or a very low cost. PaaS delivers a computing platform and software stack over the Internet that provides programmers and information technology professionals the resources they need to develop and deploy applications without the added costs and complexity of managing their own hardware and software layers on-site. Some of the biggest names in the Internet industry have noticed the demand for PaaS and now Amazon,[5] Google,[6] and Microsoft,[7] Yahoo!,[8] and others, all offer competitive PaaS services. Lastly, IaaS offers full-service virtual information stacks designed to replace a company's entire server room and network through virtualization technology.

---

[5] Amazon offers PaaS cloud computing services under the name Amazon Web Services. More information on Amazon Web Services can be found online at http://aws.amazon.com/cloudfront.

[6] Google offers PaaS cloud computing services under the name Google Apps. More information on Google Apps can be found online at http://www.google.com/apps/ intl/en/business/index.html.

[7] Microsoft offers PaaS cloud computing services under the names Microsoft Windows Azure and Microsoft Business Productivity Online Suite. More information on Microsoft Windows Azure can be found online at http://www.microsoft.com/windowsazure/. More information on Microsoft Business Productivity Suite can be found online at https://www.microsoft.com/online/business-productivity.aspx.

[8] Yahoo! offers PaaS cloud computing services under the name Yahoo! Developer Network. More information on the Yahoo! Developer Network can be found online at http://developer.yahoo.com/.

Consumers and businesses have increasingly embraced the benefits that cloud computing provides. Cloud computing services allow users more mobility and greater ability to collaborate with others. However, accompanying these advances is a grave concern over privacy: 90% of those excited for cloud computing are also concerned about data security in the cloud.[9] In order to ease these concerns over privacy and security in the cloud, ECPA's applicability to data contained in the cloud must be clarified. ECPA must be updated to give service providers clear standards on how to handle consumers' information in the cloud. Without such clarity, the skepticism of consumers, and especially enterprise users, will ultimately hinder adoption of this very valuable Internet tool.

So long as privacy rules governing the Internet remain unclear, many consumers will remain wary of adopting, or more heavily utilizing, broadband and valuable Internet-based resources. The digital age has produced an Internet that offers a wide range of valuable tools including communication, unfettered information exchange, electronic commerce, civic participation, and online tax preparation. Consumers better realize the benefits of the digital age when they fully participate in what the Internet has to offer, but if users are afraid to use their personal data online, most, if not all, of these benefits are lost.

The skepticism of enterprise users can also be damning to innovation and growth on the Internet. Enterprise users have understandably high thresholds for competitive privacy and security that serve as a major obstacle to the continued

---

[9] "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 August 26, 2010).

adoption of cloud computing services. Unless the current sense of uncertainty surrounding ECPA's application to cloud computing is cured, and adequate and clear protections are provided, skeptical enterprise users will shy away from using cloud computing services to their fullest potential. Enterprise users account for significant amounts of capital and innovative capacity. Thus, discouraging these users from fully adopting the resources offered by cloud computing drastically hurts overall Internet innovation and growth.

The conflicting, ambiguous and, at times, misguided judicial approach to the Fourth Amendment's applicability in the Internet realm highlights the importance of clarifying ECPA for the 21st Century. The Fourth Amendment has historically protected postal mail from governmental inspection during delivery. However, courts have exhibited reluctance to extend this expectation of privacy to electronic communications. While some courts have found Fourth Amendment protection for electronic communications, others have declined to do so, and the Supreme Court of the United States has punted the issue at least once. Consumers have an expectation of privacy in their communications and generally expect the same protections for e-mail as for a handwritten letter or phone call. In a world where e-mail and other electronic communications have become the norm, an absence of Fourth Amendment protections for electronic communications will shake consumer confidence and discourage broadband adoption.

Some court decisions declining to extend an individual's reasonable expectation of privacy to electronic communications highlight the troublesome judicial approach courts have taken to the Fourth Amendment in the context of the

Internet realm. In *In re Application of U.S. for Search Warrant for Contents of Electronic Mail*,[10] a federal district court in Oregon held that law enforcement officials do not have to inform an e-mail account holder of a warrant to search the contents of his or her e-mail account. Instead, the court held that notice to the Internet access provider ("IAP") was sufficient because the information sent by the subscriber passes through and may be stored on the IAP's servers. As such, the court held that the communication was no longer private information contained in the home. Similarly, in *Rehberg v. Paulk*,[11] the Eleventh Circuit held that a person loses a reasonable expectation of privacy in his or her e-mails once the e-mail is sent to and received by another party. Thus, the Eleventh Circuit found a subpoena to the subscriber's IAP for such e-mails not to violate the Fourth Amendment because the e-mails were subpoenaed directly from the IAP and not "an illegal [search of the defendant's] home computer for e-mails."[12]

On the other hand, two federal appellate courts have exhibited an understanding that makes for more appropriate national policy. In *Warshak v. U.S.*,[13] the Sixth Circuit found e-mails stored in a web-based e-mail account to be protected by the Fourth Amendment. Likewise, in *Quon v. Arch Wireless* ("*Quon I*"),[14] the Ninth Circuit found a reasonable expectation of privacy to exist in a person's text messages stored with a service provider. Although the Supreme Court of the United

---

10 *In re Application of U.S. for Search Warrant for Contents of Electronic Mail*, 665 F.Supp.2d 1210 (D.Or. 2009).

11 *Rehberg v. Paulk*, 598 F.3d 1268 (11th Cir. 2010)

12 *Id.* at 1282.

13 *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).

14 *Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008) ("*Quon I*"), *rev'd on other grounds City of Ontario v. Quon*, 130 S.Ct. 2619 (2010).

States reversed *Quon* in *City of Ontario v. Quon* ("*Quon II*"),[15] it did so on other grounds. In fact, the Supreme Court explicitly declined to address whether an employee has privacy expectations for communications made on employer-provided equipment due to a concern over the uncertain future implications of any such holding.[16] Nevertheless, although it side-stepped the issue of privacy expectations, some fear that *Quon II*'s holding that a police department's search of text messages on an employee's department-issued device was reasonable reflects a Supreme Court shying away from applying the Fourth Amendment to new technologies.[17]

Similarly, a federal district court extended to cell phone tracking a recent D.C. Circuit holding that requires a warrant for government use of GPS tracking devices to monitor individuals' movements for an extended period of time. In *U.S. v. Maynard*,[18] the D.C. Circuit held that federal agents must obtain a search warrant prior to placing a GPS tracking device on a vehicle parked on a private driveway which transmitted the vehicle's locations to federal authorities every ten seconds for a complete month. The D.C. Circuit specifically noted the extensive intrusiveness of such extended round-the-clock tracking.[19] In *In re Aplication of U.S. for Order*

---

15 *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010) ("*Quon II*").

16 *Quon II* at 2630 (2010).

17 *See e.g.* "Written Statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP, before the U.S. House of Representatives Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties," at 7, Hearing on *ECPA Reform and the Revolution in Location Based Technologies and Services*, June 24, 2010, available online at http://judiciary.house.gov/hearings/pdf/Zwillinger 100624.pdf.

18 *U.S. v. Maynard*, No. 08-3030, 2010 WL 3063788 (D.C. Cir. Aug. 6, 2010)

19 *Id.* at *12 (finding that it goes beyond the mere observation of a passerby or the following for a single journey to, "another thing entirely…to pick up the scent

Authorizing Release of Historical Cell-Site Information, the Eastern District of New York subsequently applied *Maynard*'s reasoning to reject a government request for an order directing a cell phone service provider to turn over an individual's historical cell phone location information from a two-month period.[20] Finding such cell phone tracking just as intrusive as *Maynard*'s GPS tracking, the Eastern District concluded that, "[t]he Fourth Amendment cannot properly be read to impose on our populace the dilemma of either ceding to the state any meaningful claim to personal privacy or effectively withdrawing from a technologically maturing society."[21]

A judiciary that is, at best, unsure how to apply the Fourth Amendment in the context of electronic communications highlights the need for clarity in the statutory protections ECPA provides in the electronic realm. However, the uncertainty surrounding ECPA described above has resulted in magistrate judges across the country facing difficulties with the everyday application of ECPA. At a June 24, 2010 hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the House of Representatives' Committee on the Judiciary, the Honorable Stephen Wm. Smith, a U.S. Magistrate Judge in the Southern District of Texas, testified as to problems he sees first hand in the everyday judicial application of ECPA.[22] Judge Smith's oral testimony raised two primary concerns: (1) the lower

---

again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.")

[20] *In re Application of U.S. for Order Authorizing Release of Historical Cell-Site Information*, No. 10-MJ-0550 (JO), slip op. (E.D.N.Y. Aug. 27, 2010).

[21] *Id.* at 30.

[22] Video of the House Judiciary Committee's Subcommittee on the Constitution, Civil Rights, and Civil Liberties hearing on *ECPA Reform and the Revolution in*

courts' lack of guidance from higher courts; and (2) the lack of notice provided to the person subjected to the intrusion. With regard to the lower courts' lack of guidance, Judge Smith noted that few appellate courts have actually dealt with ECPA and none have dealt with the issue of cell phone location data.

The uncertainty surrounding the Fourth Amendment and ECPA in the context of electronic communications has resulted in an unfair differential treatment of e-mail that also serves as an implicit preference for last generation hard-copy communications. Instead, a platform-neutral approach should be taken to consumers' privacy expectations in regard to their communications and electronic data. The Fourth Amendment provides greater Fourth Amendment protection to older means of communications, such as postal mail and telephone calls, while ECPA provides lesser statutory protections for e-mails. If such a framework continues, consumers will continue to rely on paper transactions in order to retain the greater privacy protections provided by the Fourth Amendment at the cost of lesser adoption of more efficient and "greener" communications technologies.

Privacy rules also need updating in order to fully appreciate the benefits of technical developments made in health-related Internet technologies ("health IT"). Health IT can provide many benefits to American patients through means of remote monitoring of and consultation with patients, collaboration amongst providers, and electronic prescriptions. These benefits are compounded in sparsely populated rural areas where patients may face great difficulties in reaching providers in

---

location Based Technologies and Services, held on June 24, 1010, can be found at http://judiciary.house.gov/hearings/hear_100624.html.

person. However, without certainty in how their most sensitive and personal medical information is treated, patients will be reluctant to utilize such beneficial technologies.

Additionally, the lesser statutory protections provided by ECPA prove arbitrary in the context of the early 21st century. The 180-day window of protection provided to e-mails may have made sense in the 1980s when e-mails were downloaded onto the hard drives of user's computers rather than left sitting passively on servers. However, today a massive reliance on web-based e-mail exists where all e-mail resides on third-party servers instead of on the user's own computer.

Lastly, even though some government agencies have set up policies providing for heightened standards for searches, ECPA still must be updated in order to provide some mechanism to ensure such policies are followed. For instance, while the U.S. Department of Justice ("DOJ") has a policy to seek prospective real-time information under a warrant standard, a recent ACLU Freedom of Information Act request shows that certain jurisdictions are using a lower standard.[23] This situation exhibits the problem of relying on agency policies: a policy is just a policy. Without updating ECPA to require the heightened standard, there is no statutory authority to point to or make that standard mandatory.

In updating U.S. privacy laws to provide legal certainty and definitional clarity for electronic communications in the 21st century, CCIA supports two general

---

[23] "ACLU Lawsuit to Uncover Records of Cell Phone Tracking," ACLU website, June 28, 2010, available online at http://www.aclu.org/free-speech/aclu-lawsuit-uncover-records-cell-phone-tracking.

propositions. First, CCIA supports the application of Fourth Amendment protections from undue search and seizure to electronic communications. Second, CCIA also supports the Digital Due Process Coalition's ("DDP") four recommendations for ECPA reform.[24]

> (1) Requiring law enforcement to obtain a search warrant based on probable cause before obtaining private communications or documents stored remotely;
>
> (2) Requiring law enforcement to obtain a search warrant before tracking people's location via cell phones or other devices;
>
> (3) Requiring law enforcement to submit proof that the information sought is relevant to a criminal investigation before electronic surveillance begins; and
>
> (4) Requiring law enforcement to submit proof that 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.

In the context of these four proposals, an exclusionary definition should be used to define what information makes up "mobile location information." Further, the definition of a "warrant" would use already existing definitions as a touchstone and notice of a warrant, with certain exceptions, would be required at a reasonable time.

---

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