

**Before the
Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
B353 Rayburn House Office Building
Washington, D.C. 20515**

HEARING ON ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

May 5, 2010

**Written Testimony
of
Albert Gidari, Partner
Perkins Coie LLP
agidari@perkinscoie.com**

Mr. Chairman and Members of the Subcommittee on the Constitution, Civil Rights, and Civil Liberties, my name is Albert Gidari and I am a partner at Perkins Coie LLP where, among other things, I represent service providers in responding to government requests for user information under the Electronic Communications Privacy Act of 1986 ("ECPA"). Thank you for the opportunity to submit this testimony concerning the need for reform of ECPA to address new innovations such as social networking, cloud computing and location-based services.

Let me say at the outset that these comments reflect my personal views and I am not speaking for or on behalf of any client or group of clients. Instead, I offer my personal observations on the state of ECPA, drawn from over 15 years of working with a wide variety of service providers, including wireless carriers, ISPs, and other online companies. Frankly, from a service provider's perspective, ECPA is broken. How the law applies to all of the new services, applications and technology available to users today is at best an educated guess. As a result, service providers are caught in the middle between law enforcement demands for ever more information and the legal imperative to protect the user's privacy.¹

ECPA reform should get service providers out of the middle. The privacy community and law enforcement may not agree on the legal standard that should apply in every case, but everyone agrees that service providers must have clear rules for disclosing user communications and information. The rules are not clear today and will be less clear tomorrow as innovation and new services arise that Congress did not contemplate in 1986 when ECPA was first passed.

The Center for Democracy and Technology's Digital Due Process Principles² (the "Principles") provide a sound basis for ECPA reform and would go a long way toward addressing what service providers want – bright line rules for disclosing user communications and information regardless of the characterization of the service, the type of technology employed, or whether the information is in transit, at rest on some computer server before reaching its intended destination or stored in the cloud. To demonstrate the need for clarity, these comments review how ECPA might or might not apply to a typical cloud computing application – the online editing and sharing of documents – and the uncertainty about the legal standards that apply to disclosure of the document and user annotations. Similarly, location based services are proliferating, but the legal standards for disclosing historical and prospective location information are a muddle at best and inconsistently applied at the state level. Finally, there are a number of steps Congress can take to improve transparency and process in ECPA to the benefit of user privacy and service provider operations. Enhanced reporting of the number of user records obtained each year, for

¹ For a detailed discussion of the serious conflicts that arise between service providers, law enforcement and users, see A. Gidari, *Keynote Address: Companies Caught in the Middle*, 41 Univ. of San Francisco L. Rev. 555 (Spring 2007).

² The Principles can be found at: <http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163>.

example, would provide the grist for better policy determinations. Likewise, service providers should be able to recover their costs of compliance, and users should be notified of legal process unless doing so would have an adverse effect on an investigation. These improvements would go far to improve ECPA.

What Rules Apply to Services in the Cloud?

Consider how ECPA might apply to a cloud computing service that permits users to create, store, edit and share documents over the Internet with others. The service is free to users, but it is advertising supported; that is, ads are served to users based on a mechanical scan of the content of the document for key words that advertisers use to display text ads. The service permits users to post documents and then invite others to view or edit them. Indeed, invited "collaborators" can annotate and edit the document in real time, seeing each others' changes as they are made.

Here's how such a service might be used today. A college student can post her paper via a cloud computing service and invite her professor to view it online. The invitation is in the form of an email generated from within the application when the student opts to share it with others. The professor can then access the document simply by clicking on the link provided in the email and then proceed to annotate the student paper, asking questions like "what is the cite for this quote?" The student may respond in real time by adding, for example, a footnote citation and inserting a comment that the citation was inadvertently omitted. The professor can see her typing as the words appear on the screen in the document itself. If the paper was a joint student project, other students could follow the real time annotations and changes. If they were offline when the changes were made, they would receive an email notice that the paper has been revised with a link to go view it.

There is substantial doubt as to whether or how ECPA applies to the service. Yet, the answer determines whether law enforcement will need probable cause and a search warrant to compel disclosure of the document and annotations or whether a mere subpoena issued without judicial review or even notice to the user will suffice. The privacy implications are palpable. If the service provider is a remote computing service to the public under ECPA, then law enforcement may compel the disclosure of the document and annotations with a grand jury or administrative subpoena with notice to the user unless such notice is delayed because it will have an adverse effect on the investigation.³ If the service provider is an electronic communication service provider to the public under ECPA, then the government must obtain a search warrant based on probable cause to compel disclosure of content in electronic storage for less than 180 days. Thus, under ECPA today, it is the characterization of the service provider and its service

³ As a practical matter, the service provider has no way of knowing whether a user has been given notice of the subpoena. Law enforcement agents are not required to certify that notice was given nor are service providers required to obtain proof of notice before disclosing the information.

offering rather than the content of the document or communication that determines the degree of protection afforded to users.

On the one hand, the student stores the document on the host's servers and uses the service's features to process her edits. The service seems to fit the ECPA definition of a remote computing service - "the provision to the public of computer storage or processing services by means of an electronic communications system."⁴ But the sharing and collaboration features of the service have more in common with an electronic communication. Indeed, the purpose of posting the document is to provide others access to it and the service provides capabilities for users to communicate within the document itself through annotations or embedded comments. ECPA defines electronic communication to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."⁵ If the service provider is wrong about how to characterize itself or the service, user information may be disclosed on a lesser standard, and the service provider may be subject to civil suit.

The risk is not theoretical. In *Quon v. Arch Wireless Operating Co., Inc.*,⁶ a case just argued before the Supreme Court on a different point of law, the service provider incorrectly decided that it was a remote computing service for purposes of disclosing stored text messages to its customer, the City of Ontario, California. The Court of Appeals for the Ninth Circuit decided that the service provider was in fact delivering an electronic communication service and therefore it needed the consent of the individual users, not the City-subscriber, to disclose the stored communications. As a consequence of guessing wrong, the service provider incurred liability.

To further confuse matters, the Department of Justice ("DoJ") takes the position that, notwithstanding the *Quon* opinion, a service provider may offer both a remote computing service and an electronic communications service simultaneously, or it may not be covered by ECPA at all. For our college student's document in the cloud, if she didn't share it with anyone and simply stored it with the service provider for her own use, presumably DoJ likely would view the service as a remote computing service. But because the service provider is permitted to access the content of the document for advertising purposes, DoJ would say that ECPA does not apply at all to the service. The document simply falls outside ECPA and a simple subpoena without any notice to the user would suffice to compel its disclosure.

⁴ 18 U.S.C. § 2711(2).

⁵ *Id.* § 2510(12).

⁶ 529 F.3d 892 (9th Cir. 2008).

It is unclear whether DoJ would agree that the collaboration and sharing features of the service that permit users to communicate with each other within the document itself constitute an electronic communication service. But even if it did, once the annotations were read by any other person authorized to view them, DoJ's position would be that ECPA no longer applies, just as it contends ECPA does not apply to opened email.⁷

So what is a service provider to do? CDT's Principles would treat user generated and stored content the same regardless of the service, functionality or technology involved. The Principles would require the government to obtain a search warrant based on probable cause to compel disclosure of any content stored in the cloud. This approach has the virtue of assuring users that their information will be protected the same in the cloud as it would be on their own computer in their home. Service providers would have a clear rule that would be easy to follow, and litigation would be avoided. In practice, some service providers already take this position and any applications that permit users to share content are treated as electronic communication services.

What ECPA Issues Arise with Location Based Services?

Location information long has been a mainstay in criminal investigations, yet after almost two decades of acquisition and use of the data, the legal standard for obtaining historical location information records, current real time location, and prospective tracking remain unsettled. Whether probable cause is the appropriate standard for obtaining historical location information is before the Court of Appeals for the Third Circuit,⁸ but plainly, the government routinely acquires historical data using the lower standard in Section 2703(d) of Title 18.

The legal standard for obtaining prospective location information and tracking data has been the subject of a "magistrates' revolt" for several years. Many federal magistrates have refused to permit prospective location information acquisition on less than a probable cause showing. Those magistrates who reject the lesser standard find that when the government uses a cell phone to track a user, it converts the phone

⁷ The DoJ steadfastly maintains that once an email has been opened, it is no longer in electronic storage and can be obtained with a subpoena. The Court of Appeals for the Ninth Circuit has rejected this interpretation, but DoJ disagrees and routinely moves to compel service providers who reside in the Ninth Circuit and store user data within that jurisdiction to disclose such information in districts outside the Ninth Circuit states. Just last month, DoJ moved to compel Yahoo to make such a disclosure in the United States District Court for the District of Colorado, but subsequently withdrew its demand. An amicus brief filed in the case can be found at: <http://www.eff.org/files/filenode/inreusaorder18/AmiciBriefYahooEmails.pdf>.

⁸ *In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp. 2d 585 (W.D. Pa. 2008)(entire district rejects government request and requires probable cause for stored and prospective location), *order aff'd by In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008).

into a mobile tracking device, which is governed by Section 3117 of Title 18 and which, pursuant to Federal Rule of Criminal Procedure 41, requires a search warrant based on probable cause.

But sometimes even in the same judicial district, some magistrates have ruled that the government is entitled to the information on a lesser showing. Because a single district judge's ruling does not establish binding precedent within a district,⁹ service providers must follow whichever form of order they receive. And because ECPA provides the floor for state legal process as well, the proper legal standard is more confusing when federal magistrates sitting in the same federal district in a state disagree – which standard should a state court judge follow when issuing a tracking order? The result is that two identically situated users under investigation in the same state may have their location information acquired by federal agents on two different standards, and for state investigators, it essentially is a dealer's choice as to which standard is applied to get the tracking information.

As interesting as the debate is over the proper legal standard for tracking, there are other legal issues not answered in ECPA today as well. The following issues are faced by service providers every day in response to government demands for acquisition and use of location information:

- a. **Duration and Periodicity of Order.** Orders for location information seldom state the duration. If Rule 41 applied, the duration would be 10 days; but common practice is to require location information reporting for the duration of a pen register order, up to 60 days. Further, how frequently location information is to be acquired during the course of a day remains unclear and whether it is to be limited to the beginning and end of a call, or autonomous registration. In other words, can law enforcement require reporting of location information every 15 minutes for a period of 60 days?
- b. **Compensation to Service Provider.** Under the government's hybrid theory, service providers should be entitled to cost recovery under both Sections 3124 and 2706 of Title 18, but there is no clear reimbursement rule for Rule 41.
- c. **Notice to Users.** Notice is not prohibited for historical records obtained by a court order alone under Section 2703(d); it is prohibited for hybrid order; and it is unclear for Rule 41.
- d. **Target v. Associates (hub and spokes).** Regardless of the legal standard applicable to the target phone, what standard applies to obtain the location information for all those with whom the target communicates? It is common in hybrid orders for the government

⁹ See, e.g., *ATSI Communs., Inc. v. Shaar Fund, Ltd.*, 547 F.3d 109, 112 & n. 4 (2d Cir. 2008) (citing cases).

to seek the location of the community of interest – that is, the location of persons with whom the target communicates.

- e. Customer or User Consent to Track/disclose (implied or express). Can a user consent to tracking or disclosure of location information, and if so, whose consent is necessary – the user's or subscriber's?
- f. Preemption of less strict state law. To the extent a state law or rule permits location information to be disclosed on a lower than federal standard, ECPA preempts the state rule, but state law enforcement authorities disagree or seldom have heard of ECPA.
- g. GPS standard. The accepted rules of *Knotts*¹⁰ and *Karo*¹¹ -- tracking in a public place is permissible without a warrant; tracking in the home is not -- are under attack in state courts as those rules have been applied to GPS.¹² Courts are now deciding that modern GPS is much more intrusive than the "bugs" used in *Knotts* and *Karo*, and such sensory enhancements may require reevaluation in light of the Supreme Court's decision in *Kyllo*.¹³ GPS is now part and parcel of many third party applications as well -- what standard applies to GPS data in a third party's possession?
- h. Location information as content. In the case of many location-based services ("LBS"), some logging of a user's location may occur and be retained. In many such applications, the user is conveying his or her location to another user essentially as a communication – "here I am." LBS providers treat such electronic communications as content that cannot be disclosed under ECPA without complying with the requirements of Section 2703, which means that the characterization of the service provider as a remote computing service or an electronic communication service will determine the standard under which the location information is disclosed.

¹⁰ *United States v. Knotts*, 460 U.S. 276 (1983) (Fourth Amendment does not prohibit tracking in a public place).

¹¹ *United States v. Karo*, 468 U.S. 705 (1984) (monitoring a beeper in a private home violates the rights of those justifiably expecting privacy there).

¹² See *People v. Weaver*, <http://www.nycourts.gov/ctapps/decisions/2009/may09/53opn09.pdf> (N.Y. Court of Appeals, May 12, 2009).

¹³ *Kyllo v United States*, 533 U.S. 27 (2001) (use of thermal-imaging device to detect relative amounts of heat in the home is an unlawful search).

How Can Greater Transparency be Achieved in ECPA?

Service providers are overwhelmed by the volume of governmental requests for user communications and information. There are over 10,000 federal, state and local governmental agencies with subpoena power. The volume of user information collected by government is astonishing, but largely unreported. Only Google publicly reports the number of governmental requests it receives.¹⁴ The number of requests Google receives is dwarfed by the number of requests wireless carriers receive each year.

It is difficult to understand how sound policy can be made without knowing how much user information is collected. Take pen register information for example. DoJ is required to report the number of pen registers conducted each year to Congress.¹⁵ It has not done so with any regularity, but even if it had, the number of pen register orders implemented is not all that revealing. More important is the number of subscriber records obtained under the order.

Pen register orders routinely authorize the investigating agent to compel disclosure of subscriber records for every person called or calling the target phone. A target can make hundreds of calls during a typical 60-day pen register period. The pen register yields a list of numbers, and law enforcement agents routinely send that list to every carrier that might possibly provide service, demanding production of any records for any number that belongs to that carrier. Thus, a single pen register order can result in the disclosure of hundreds of individual customer phone records. Likewise, a single grand jury subpoena may list dozens of accounts for which subscriber information is sought.

Account-based reporting would provide Congress and the public with the necessary information to judge whether the right balance has been struck as to the standards and ease with which information is

¹⁴ See the Google Reporting Tool at <http://www.google.com/governmentrequests/>.

¹⁵ See 18 U.S.C. § 3126. Reports concerning pen registers and trap and trace devices.

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include information concerning—

- (1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- (2) the offense specified in the order or application, or extension of an order;
- (3) the number of investigations involved;
- (4) the number and nature of the facilities affected; and
- (5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

gathered. Congress has required as much for emergency disclosures, but again, no public reports are available as to whether DoJ has complied with this requirement either.¹⁶

Service providers are prohibited by ECPA from recovering the cost of producing phone records,¹⁷ but service providers otherwise may recover costs reasonably necessary for the production of other subscriber information. When records are "free," such as with phone records, law enforcement over-consumes with abandon.¹⁸ Pen register print outs, for example, are served daily on carriers without regard to whether the prior day's output sought the same records. Phone record subpoenas often cover years rather than shorter, more relevant time periods. But when service providers charge for extracting data, such as log file searches, law enforcement requests are more tailored. Further, mandatory reimbursement would permit Congress to "follow the money," creating an audit trail of how much is spent in collecting user communications and information.

Users, of course, generally are unaware of requests for their information. The law precludes notice of interception and pen register orders, but there is no prohibition on notice of grand jury or administrative subpoenas or other court orders. Yet, because ECPA does not require notice to the user prior to service provider disclosure to the government, most service providers do not give notice.

The government has the ability to obtain an order to prevent notice in limited cases where such notice may yield an adverse result such as (a) endangering the life or physical safety of an individual; (b) flight from prosecution; (c) destruction of or tampering with evidence; (d) intimidation of potential witnesses; or (e) otherwise seriously jeopardizing an investigation or unduly delaying a trial.¹⁹ But more commonly, it simply requests nondisclosure (although some have argued that disclosure would be an obstruction of justice), and service providers generally comply.

But the government has a means to ensure against an adverse effect on an investigation. Mandatory notice should be required in all other cases so that users (rather than service providers) can assert their

¹⁶ See 18 U.S.C. § 2702(d) Reporting of emergency disclosures.--On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where--

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

¹⁷ See 18 U.S.C. § 2706(c).

¹⁸ No one knows how long the collected information is retained or which agencies have access to it.

¹⁹ 18 U.S.C. § 2705.

rights. How would a service provider know that an otherwise routine-looking subpoena was directed at protected First Amendment rights for example? Service providers should not be in the middle of such disputes.

Finally, service provider response to the enormous volume of government requests is an exercise in daily triage. Every agency believes its request should be handled first, its investigation is most important, and any other agency's needs can be given lower priority. It is not uncommon in pen register orders today to see a requirement to produce subscriber records "immediately" upon agency request or in an expedited fashion such as "no later than 3 days after demand." Rules of procedure typically allow only a short period of time in which to respond, and put the burden on the third party to move to quash or amend an unduly burdensome request.

This "press for production" establishes all the wrong incentives. There should be no incentive to rush or not review legal process. Moreover, the squeaky wheel should not get the oil of advanced or quicker production by calling security office personnel and threatening contempt or cajoling early compliance. The service provider ought to have, and ECPA should provide, a priority rule of "first in, first out" for any request, and a uniform time frame for compliance of 30 days should be set for both federal and state governmental entities, absent an emergency.

Conclusion

Thank you for the opportunity to present these comments today in favor of ECPA reform. ECPA always has been a complicated statute and difficult for service providers to implement in the simplest of times. But as new services and innovations come along, the task of legal compliance has become more luck than art. Service providers want clarity and bright line rules. I believe that users, privacy advocates and law enforcement want the same thing.

In closing, the Committee should understand one thing – service providers employ hundreds of security office professionals who each day confront ECPA problems of interpretation and implementation. These men and women know that their hesitation or delay may have life or death consequences. At the same time, they know that user privacy is important and an imperative. It is really these men and women who are caught in the middle and deserve our appreciation for the professional job they do every day.

Similarly, law enforcement agents who seek user communications and information generally do so in a professional and courteous way. By far, the majority of requests are handled in this way and do not give rise to disputes. While the relationships between law enforcement and service providers may vary from provider to provider, in my experience, mutual respect and professionalism has been the rule.