Written Statement of Marc J. Zwillinger

Partner

Zwillinger Genetski LLP

U.S. House of Representatives Committee on the Judiciary

Subcommittee on the Constitution, Civil Rights, and Civil Liberties

Hearing on

ECPA Reform and the Revolution in Cloud Computing

Washington, D.C.

September 23, 2010

Chairman Nadler, Ranking Member Sensenbrenner and Members of the Subcommittee,

Thank you for having me back to testify about ECPA reform and specifically about the issues relating to cloud computing, which make up a large component of my legal practice. As the committee knows, I worked as a Trial Attorney in the United States Department of Justice Computer Crime and Intellectual Property Section from 1997-2000, and for the last ten years I have been representing companies, including internet service providers, social networking companies, and wireless providers on issues related to the Electronic Communications Privacy Act ("ECPA"). In my career, I have taught hundreds of law enforcement agents how to apply ECPA and hundreds of compliance paralegals at leading Internet providers how to respond to law enforcement requests for data. I have also litigated ECPA-related issues in federal district and appellate courts. As an adjunct professor at the Georgetown University Law Center in Washington, D.C., I have taught courses covering ECPA. I have also been involved in the Digital Due Process Coalition effort for the last 2 years. I am testifying today solely in my individual capacity and not on behalf of any clients or the Digital Due Process Coalition.

As someone who deals with the real world application of ECPA on a daily basis, I am acutely aware of the strengths and the failings of the statute. Although each of the proposed areas for ECPA reform are important, the most pressing area for legislative action relates to the storage of user data with third party Internet providers, often referred to as storage "in the cloud."

As the testimony from industry representatives will likely make clear, Internet companies are struggling to apply the existing and somewhat outdated categories of information protected by ECPA to their products and services. Back in 1986 when ECPA was passed, companies may have been outsourcing the processing of certain data, but not on the same scale as today. Moreover, individuals were not using third-party services like Yahoo! Mail, Google Documents, or Flickr to store their most private correspondence, writings and photos, nor were they communicating regularly through social networking services. The increasing use of the Internet as a primary repository for users' private documents has made the issue of privacy and law enforcement access to such materials of significant importance to individuals who use the services, companies that offer the services, and to law enforcement. Given the widespread use of cloud computing by U.S. citizens and businesses, the laws governing access to user data should be clear and easy to apply. The Stored Communications Act ("SCA") is exactly the opposite. In fact, the distinctions and categorizations contained in the 1986 statute often make little or no sense in today's environment. Through my testimony, I intend to explain five fundamental problems with how the SCA applies to cloud computing and why this Committee should consider passing new legislation to address these issues.[1]

[1] Four of the five issues are addressed in the Digital Due Process ("DDP") principles. The issue that is not addressed pertains to access to communications by non-government actors, such as civil litigants and criminal defendants.

1. **For materials such as emails or private messages that are intended to be the most protected, the definition of "Electronic Storage" is difficult to apply.**

Take a moment to consider the types of emails that are in your own inboxes. If you are a typical email user, the emails or private messages that are both the most important and the most private are the older messages that you have read through several times and have intentionally decided to save. These emails might include treasured notes from a spouse, a child, or a close friend. By contrast, the unopened emails in your inbox are likely to be commercial solicitations that you have not yet had time to delete. Unfortunately, under the current structure and interpretation of the Stored Communications Act ("SCA"), the latter messages are clearly protected from government access except when law enforcement obtains a search warrant. The protection for the more important messages – the ones you purposely chose to save – however, is much less certain or is insufficient. Let me explain why.

The SCA affords the highest protection to materials that are in "electronic storage" for 180 days or less by preventing the government from accessing these types of communications without a search warrant. The SCA defines "electronic storage" as "(A) any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. . . . " 18 U.S.C. § 2510(17). Email communications meeting either condition (A) or (B) and that are less than 181 days old are protected from disclosure to anyone except to the government pursuant to a search warrant.

Under this definition of "electronic storage," the Department of Justice has taken the position that a search warrant is required only for messages that have never been read or opened by a user. This argument is based on the theory that when an email has been downloaded to a user's computer, the storage by the ISP is no longer temporary or intermediate, because a copy of the message has been delivered to the user.

When the SCA was passed in 1986, this type of distinction may have made some sense. In the 1980s, ISPs would store user email on their systems only briefly until the user connected to the ISP and downloaded the mail. That brief storage was temporary and intermediate, as described in the definition of electronic storage. Today, however, webmail is the predominant form of personal email communication and webmail is seldom delivered to a user for local storage on his or her own PC.[2] Rather, it stays in the cloud and the user interacts with the mail on the provider's servers. The ability to access webmail from mobile devices and portable computers is one of the chief advantages of webmail and is one reason why webmail has come to dominate the non-business user email market. But for webmail providers, there is no longer any "temporary intermediate" storage in the manner initially contemplated by the statute. Rather, whether or not a user reads an email, it will continue to be stored in the cloud forever—or at least so long as the user's account is active. Thus, the act of "reading" the email is of no legal moment, because it does not transform the storage from "temporary" to

[2] If webmail resides on a user's computer at all, it is in a temporary web-browsing cache.

permanent. Nor does the user's action or inaction have any impact on the physical location of the email – it remains on the provider's servers and is not downloaded to a computer that is within the realm of what is covered by the user's Fourth Amendment rights.

Over DOJ's objection, the Court of Appeals for the Ninth Circuit extended the definition of electronic storage to all emails stored by an ISP – whether read or unread – under the theory that even after any "temporary" period of storage has ended, any further storage by the ISP is within the backup prong of the definition of electronic storage because it is a "backup" for the user.[3] This is the correct outcome as a policy matter – the statutory protections for email should not vary depending on whether the email has been delivered or read, yet, the Department of Justice takes issue with this position and continues to seek to compel the production of opened mail by subpoena in all judicial districts except the Ninth Circuit.[4] In fact, earlier this year I was poised to litigate this issue against the U.S. Attorney's office in Colorado after it moved to compel Yahoo! to respond to a subpoena for emails that were less than 180 days old but which the user had not read. After Yahoo! filed its opposition to the motion to compel and amicus briefs had been submitted supporting Yahoo!'s position, the government withdrew its motion.

Lest any future courts accept the Department's position, the SCA should be amended to remove any question that the standard the government has to meet in order to access email is not dependent on whether the email is opened or unopened.

2. The 180 day rule is arbitrary and based on a false assumption

Like the purported distinction between opened and unopened mail, the provision in ECPA that automatically diminishes a user's protection vis-a-vis the government as email ages is arbitrary and irrational. Under the SCA, private messages or emails 180 days or older may be obtained by the government with a mere subpoena or a § 2703(d) order with prior notice, unless such notice is authorized to be delayed. However, law enforcement must obtain a warrant to obtain emails stored with a provider for 180 days or less. This may have made sense in 1986, but it is no longer rational, much less compelling.

At the time ECPA was passed in 1986, data sent through an electronic communication system was not stored by the provider for long periods of time.[5] Thus, if not already deleted by the ISP, any data stored for more than 180 days was not deemed to be the type of data worth protecting. Emails over 180 days old were likely unread emails that no user had bothered to retrieve and download to their own computer – probably most often associated

[3] *See Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003).

[4] *See* U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence Manual,* Chap. 3, a 2009 edition, found at www.cybercrime.gov/ssmanual/03ssma.htm); *United States v. Weaver*, 636 F. Supp. 2d 769, 772-73 (C.D. Ill. 2009). The government also believes that the "backup protection" reference in the statute refers only to backups created by the mail provider.

[5] *See* H.R. Rep. No. 99-647 at 65 ("Most—if not all—electronic communication systems (such as electronic mail systems), however, only keep copies for a few months.")

with dormant or abandoned accounts. In fact, it was expressly assumed that storage of that duration would make the private email more akin to a business record of the ISP than content belonging to the user.[6] The intervening years, however, have proven that the original assumption was incorrect. Online storage services for all types of communications, including music, files, photos, and emails, have become the rule and storage capacity in the cloud is virtually unlimited with little or no financial cost to the user. Thus, a user who stores online content for more than 180 days, is now more, not less, likely to have a strong interest in that data, and no one would consider such data to be merely a business record of the ISP. Yet the Stored Communications Act still contains the original arbitrary six month dividing line for privacy protection such that even materials that are obtainable only through a search warrant for the first 180 days of their existence become obtainable via a subpoena (with prior or delayed notice) on the 181st day. This is true despite the fact that it remains a criminal offense for a third party to hack into an email system and obtain access to the same message regardless of its age.[7] This arbitrary time limit on privacy should be eliminated.

3. Congress intended content to be more protected than transactional records in theory, but in practice content does not get enough protection.

Lawyers who work regularly with ECPA generally describe the statute as providing greater protection for content, like photos, than for transactional or subscriber records, like log files. This can be clearly seen by the fact that the highest level of protection under the SCA is reserved for the contents of communications in electronic storage and the lowest for certain limited types of basic subscriber records that are identified in 18 U.S.C. § 2703(c)(2), which consist of: name, address, telephone records, length and type of service, other subscriber number or identity including any network address, and means and source of payment.

Of the two other categories in the SCA, the protection for the contents of communications stored by a remote computing service was intended to be at least as robust, if not more, than the protection provided to transactional records. This is not, however, the way ECPA works in practice. When Congress passed ECPA, it expected that the means by which the government would get access to the types of private content not deemed to be "in electronic storage" – such as files stored with a remote computing service – was through a court order under 18 U.S.C. § 2703(d) or a subpoena with prior notice to the user. With such prior notice, a user would know of the request for his or her documents and would have the opportunity for prior judicial review before the contents of the account were turned over – either by the court who initially issued the order, or subsequently if the user challenged the request. The delayed notice provisions of 18 U.S.C. § 2705 were intended to be used sparingly, as the requirement of prior notice to the subscriber was identified as an important statutory protection provided to

[6] *See id.,* ("To the extent that the record is kept beyond that point it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.")

[7] *See* 18 U.S.C. § 2701.

the user.[8] By contrast, when requesting transactional data or subscriber data not specifically listed in § 2703(c)(2), the government was not required to give user notice, even though the same basic showing was required.

But, in modern law enforcement practice, it often works the opposite way – transactional data receives more protection than the contents of files stored by a remote computing service. By regularly relying on the exception in the SCA that allows it to delay notice to the subscriber whenever there is a "written certification of a supervisory official" that providing notice would have an adverse effect on the investigation, the government can obtain contents of stored files with a subpoena, when transactional records require a court order under § 2703(d). And users whose content is sought by subpoena have no opportunity to challenge the request before production. As a result, contents of files and messages – except those that are in electronic storage for 180 days or less – are easier to obtain than transactional records. This switch in protection from the way ECPA was originally designed is significant in light of the vast amount of user data that is currently stored in the cloud.

In revisiting ECPA, Congress should make clear that a subpoena with delayed notice is not an acceptable way to access the contents of any private stored content belonging to a user by requiring the government instead to demonstrate probable cause before gaining access to such content.[9]

4. The SCA is not technology neutral

One reason why the standard for law enforcement access for private stored content should be reevaluated is to make the SCA truly technology neutral. When choosing between storing documents locally on an individual's own PC, or using a password-protected storage service in the cloud, the key considerations should relate to efficiency, accessibility, security and cost, not law enforcement's ability to access the data from a third party. That is not the situation today. The SCA pushes a personal or business user seeking to protect his or her data from access by third-parties, including the government, towards choosing a local storage option to maximize the protection for the data. If a business owner stores confidential files on a local server, the government must either execute a search warrant or serve a subpoena for the documents, allowing the personal or business user who receives the subpoena to have an opportunity to object to the subpoena or assert relevant privileges. By contrast, if those same files are stored with a third-party provider in the cloud, the government could serve a lesser form of process on the provider with delayed notice and prevent the business owner from learning the documents had been subpoenaed until after they had already been provided to the government.

[8] See H.R. Rep. No. 99-647 at 68 ("[T]he purpose of such notice is to provide the subscriber or customer with an opportunity to contest the propriety of such a disclosure.")

[9] One district court has already held that SCA violates the Fourth Amendment by permitting the seizure of emails without a warrant and without prior notice to the subscriber on less than a showing of probable cause. *Warshak v. U.S.*, No. 1:06-CV-357, 2006 WL 5230332 (S.D. Ohio July 21, 2006), *vacated in part on other grounds*, 532 F.3d 521 (6th Cir. 2008).

The purported justification for decreased privacy protection where the documents are hosted in the cloud is the third-party doctrine: that documents that a user has knowingly shared with a third-party are understood to be less private. But that assumption is flawed in several respects. First, as a practical matter, documents stored in the cloud may be more secure than documents stored on a local server. For example, third-party technology providers generally spend more time and resources securing data than the average user does on his or her home PC where they may be unprotected from intrusion or secured only by a firewall that the user is not particularly adept at configuring, without an intrusion detection system or 24 hour monitoring. Second, by storing data on password-protected third party systems, users are not generally providing the third party with any broad right to review, access or disclose the data for its own purposes. In fact, the third-party generally has limited rights to automatically screen data for harmful or malicious content that may cause damage to their network, and no rights to access the private files. Thus, users should not be considered to have waived the confidentiality of private documents by hosting them in the cloud. In fact they may be enhancing their confidentiality compared to storing them on a home PC where other household members could view them when using the computer. Consequently, as a policy matter, there is no legitimate reason for U.S. law to provide more robust privacy protections for users who elect local storage over secure storage in the cloud.[10]

5. The complete silence on access by civil litigants, criminal defendants and estates of deceased users creates uncertainty and unnecessary litigation

An often overlooked but increasingly important issue associated with the application of the SCA is access by civil litigants, criminal defendants and estates of deceased users. In the course of representing Internet service providers, I have witnessed firsthand the confusion that is the result of the absence of guidance in the SCA regarding access by civil litigants and criminal defense counsel and how frequently ISPs receive unlawful subpoenas seeking to compel production of the contents of Internet communications.

The SCA contains clear and unequivocal prohibitions on disclosure of both types of content records that may be in the possession and control of a third-party ISP: materials in "electronic storage" and "contents of wire or electronic communications in a remote computing service." There are eight specific exceptions to these prohibitions that provide specific avenues for disclosure to government entities, disclosures based on consent, or disclosures by the ISP in order to render service or forward communications. However, there is not a single provision that authorizes any type of disclosure of customer communications in response to legal process issued by a civil litigant or criminal defendant. [11]

---

[10] Certainly, there are circumstances where data stored in the cloud is made less private because it is shared with multiple users, just as data within a local work environment may also be shared with multiple users. The test, however, should be applied neutrally whether the storage is local or in the cloud.

[11] *See O'Grady v. Superior Court*, 139 Cal. App.4th 1423 (2006); *Crispin v. Christian Audigier, Inc.*, __ F. Supp. 2d ___, 2010 WL 2293238 (May 26, 2010); *Flagg v. City of Detroit*, 252 F.R.D. 346, 366 (E.D. Mich. 2008); *Viacom Int'l v. YouTube*, 253 F.R.D. 256 (S.D.N.Y. 2008); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611-12 (E.D. Va. 2008).

When ISPs inform civil litigants and criminal defendants, as they must, that federal law precludes them from disclosing the communications without the consent of the author or recipient; they invariably meet resistance and are sometimes forced to litigate these issues. Even judges are astounded that they have not been given the power, under any circumstances, to require the production of email content by an ISP in a civil case. In recent years, the storage of increasing amounts of content in the cloud has only increased the importance of addressing these issues.

The problem is even more complicated when a criminal defendant seeks information, where this lack of access may lead to due process concerns. Because ECPA contains a flat prohibition against the disclosure of contents of communications to non-governmental entities, criminal defendants have no mechanism to obtain emails even when there is no subscriber who can consent to the disclosure. One solution is to rely on law enforcement to request the data on a criminal defendant's behalf, but in some cases, defense attorneys are unwilling to disclose their defense strategy to the government and in others, the prosecutors are unwilling to cooperate. Judges, for their part, can be reluctant based on separation of power issues to require the government to use its investigative powers at the behest of a defendant to retrieve the materials. And the third-parties who sent or received these emails may be unwilling or unable to consent to their disclosure.

For this reason, some trial courts in California have issued bench orders and oral rulings finding that the restrictions in ECPA threaten to interfere with the defendant's constitutional rights to due process and effective assistance of counsel. Furthermore, civil litigants are equally stymied by the prohibitions of the SCA. Although many problems are solved by requiring the civil party to serve their discovery subpoena on the third-party who is the account holder, rather than the ISP, there are some circumstances where the account holder is a third-party who is not within the court's jurisdiction, or is unable to access their account to obtain the emails, or is deceased. These situations often lead to litigation. I am currently involved in a case in Massachusetts where my client has been sued for a declaratory judgment to declare that the emails in a deceased user's account should be turned over as property of the estate. Even if the plaintiffs succeed in invalidating the 'no right of survivorship' clause in the contract, the ISP would be barred under ECPA from disclosing the contents of the emails, and would be forced to appeal the decision.

ECPA clearly needs an escape valve of some sort to allow for disclosure of the contents of communications or stored files in very limited and narrow circumstances. I have previously proposed the text of such an escape valve in a law review article[12] about the SCA in 2007, whereby a criminal defendant or civil litigant would be able to seek a court order to obtain

---

[12] Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not A Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569 (2007).

stored content after making a rigorous showing that other methods of gaining access to the data have been unsuccessful, that the information is relevant and material to the case and that the subscriber/user and the ISP have been given notice and an opportunity to be heard. I continue to believe the addition of such a provision would reduce some of the confusion and unnecessary litigation generated by the current law.

ECPA has functioned fairly well during its first 20 years in striking the right balance between law enforcement needs and the privacy expectation of U.S. citizens. But when it was initially passed in 1986, Congress recognized that the "law must advance with the technology to ensure the continued vitality of the fourth amendment."[13] Based on my experience as an ECPA practitioner for the past 13 years, I believe the time is ripe for another advancement. I hope you will consider these perspectives in crafting legislation that balances law enforcement needs and user privacy in a manner that reflects the reality of the uses of the Internet in the 21st century and no longer relies on outdated assumptions.

Thank you for the opportunity to testify today. I would be pleased to work with the Committee in more detail as the ECPA reform process moves forward.

[13] . S. Rep. No. 99-541, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559.