United States House of Representatives
Subcommittee on Crime, Terrorism,
Homeland Security and Investigations

"ECPA Part 1: Lawful Access to Stored Content"

Tuesday, March 19, 2013
2141 Rayburn House Office Building, 10:00 a.m.

WRITTEN STATEMENT OF ORIN S. KERR
FRED C. STEVENSON RESEARCH PROFESSOR
GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

It is my pleasure to testify this morning about the Electronic Communications Privacy Act ("ECPA"), and specifically about the provisions of ECPA that regulate government access to stored contents held by Internet providers. In my view, these important provisions are badly flawed and badly outdated.

My testimony will focus on five major problems with the statute governing access to stored contents under ECPA. First, the statute provides very weak protection for contents of communications held for more than 180 days. Second, the statute appears to offer no protection for search engine queries. Third, the scope of the statute's warrant protection is uncertain. Fourth, part of the existing statute does not satisfy the Fourth Amendment. And fifth, the statute imposes no requirements of minimization, particularity, or non-disclosure for contents obtained under its provisions.[1]

These five problems point to a pressing need for Congress to revisit ECPA's provisions on lawful access to stored contents. My testimony will begin by summarizing the existing provisions of the law as they were enacted in 1986. I will then turn to the five major problems with those provisions from the perspective of 2013.

[1] Parts of my testimony are adapted from a forthcoming article on ECPA reform that will be published in Volume 162 of the *University of Pennsylvania Law Review.*

Understanding ECPA's Current Provisions on Compelled Access to Contents of Communications

The provisions of ECPA governing lawful access to stored content are found in 18 U.S.C. § 2703(a)-(b), which was enacted in 1986. These provisions create statutory privacy rights for "subscribers or customers" of two kinds of computer network services that existed at the time. The first kind of service is an "electronic communications service" provider ("ECS"), which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Translated into plain English, an ECS is any service that provides connectivity, e-mail, or text messaging services. 18 U.S.C. § 2703(a) identifies the rules that the government must follow to compel contents of communications held by ECS providers. According to its provisions, the government needs a warrant to compel contents from an ECS provider if the contents have been stored for 180 days or less. If the contents have been stored for more than 180 days, however, the government can use lesser process pursuant to 18 U.S.C. § 2703(b).

The second type of Internet service regulated by the law is a "remote computing service" ("RCS"), defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). In layman's terms, an RCS is a remote storage service that any member of the public can use, such as a cloud storage service. 18 U.S.C. § 2703(b) offers three ways that the government can compel contents held by an RCS or contents held by an ECS for more than 180 days. First, investigators can use a subpoena with either prior notice or delayed notice. Second, investigators can use a "specific and articulable facts" court order under 18 U.S.C. § 2703(d) with either prior notice or delayed notice. Third, investigators can use a warrant to obtain contents and do not need to satisfy a notice requirement.

Problem 1: No Warrant Protection for Storage More Than 180 Days

The current language of 18 U.S.C. § 2703(a)-(b) has five major problems. The first problem is that the statute does not require a warrant for remotely–stored contents held for more than 180 days. The government can compel contents held for more than 180 days with a mere subpoena. This is a strange result because most people use their e-mail accounts as a permanent storage site akin to a virtual home online. According to one recent report, a typical

user of the popular Gmail e-mail service stores more than 17,000 e-mails in her account at any given time.[2] Almost 12,000 of those e-mails are received e-mails stored in the inbox, and almost 6,000 are sent e-mails directed elsewhere.[3] It is likely that most of those communications have been stored for more than 180 days. Under ECPA, however, only e-mails stored 180 days or less can receive statutory warrant protection. Anything stored for a longer time can be accessed by the government without a warrant. I find that aspect of the statute impossible to justify. It is a puzzling result that makes no sense for today's Internet and today's Internet users.

Problem 2: No Protection for Search Engine Requests

A second problem with the current statute is that private communications held by Internet services that do not fit within the definition of ECS or RCS receive no protection at all. Search engine requests provide the most important example. According to one study, search engines analyzed about 18.4 billion search requests from the United States in the month of March 2012 alone.[4] Search engine requests can reveal a person's innermost thoughts, and as a result such requests contain highly sensitive information. But it appears likely that search queries stored with services like Google are not protected under current law because they provide neither ECS nor RCS.

Search engines plainly do not provide ECS. They are destinations for communications, not providers of connectivity or messaging. And search queries do not appear to provide RCS, either. Recall that a remote computing service is defined by ECPA as a service that provides the public "computer storage or processing services by means of an electronic communications system."[5] Users do not send their search queries to search engines for storage purposes. Storage is a bug for users, not a feature. Whether ECPA protects search queries therefore hinges on whether search engines provide "processing services." The relevant text and legislative history suggests that they do not. In the

[2] *See* Mike Barton, *How Much Is Your Gmail Account Worth?*, Wired, available at http://www.wired.com/insights/2012/07/gmail-account-worth/

[3] *See id.*

[4] *See* Press Release, *comScore Releases March 2012 U.S. Search Engine Rankings*, http://www.comscore.com/Insights/Press_Releases/2012/4/comScore_Releases_March_2012_U.S._Search_Engine_Rankings

[5] 18 U.S.C. § 2711(2).

context of computer data, the word "process" suggests operations on that data rather than a response to a query. The Senate Report accompanying ECPA clarifies the point: remote processing meant the outsourcing of tasks, such as number-crunching, that a computer of the 1980s might not be able to complete easily.[6] Search engines do not appear to fit the mold, as users do not use search engines as substitutes for the storage or processing powers of their own machines. For those reasons, it appears that likely that search engine queries are not protected by current law. The issue is not free from doubt, and courts have not ruled definitely on the issue.[7] But it appears that likely that search queries receive no statutory protection at all from the compelled storage provisions of ECPA.

Problem 3: The Scope of the Warrant Requirement Is Uncertain

A third important problem with the current statute is its uncertain scope. The most important example is opened e-mail stored for 180 days or less. Courts are presently divided on whether opened e-mails stored on a server will generally be covered by the ECS rules (which require a warrant) or the RCS rules (which do not). The source of the difficulty is the complex definition of "electronic storage" in 18 U.S.C. § 2510(17), which is critical because

---

[6] The Senate Report accompanying the passage of ECPA offered the following explanation of the concept of a "remote computing service" :

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer.

S. Rep. No. 99-541 (1986), at 10-11.

[7] Notably, Google has claimed that its search engine queries are covered by ECPA on the ground that it provides RCS. In litigation over the disclosure of Google search queries, Google made the following argument that its services are protected by the SCA:

> Google processes search requests as directed by, and for, its users who in turn retrieve the search results of their choosing from Google's index, or Google sends the results by email or text messages to individuals, to wireless phones or other designated mobile devices. Said in plain language, users rely on the remote computer facilities of Google to process and store their search requests and to retrieve by electronic transmission their search results.

See Google's Opposition to the Government's Motion to Compel in Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006), available at 2006 WL 543697.

only contents in "electronic storage" receive ECS protections. Some courts read the definition to include opened e-mails in the statute's ECS coverage on the theory that they are copies of e-mails stored "for backup purposes" under § 2510(17)(b). *See Theofel v. Farey–Jones*, 359 F.3d 1066, 1075-76 (9th Cir. 2004). On the other hand, other courts have concluded that opened e-mails are not covered by the ECS rules but rather are covered under the RCS rules on the theory that a user stores opened e-mails like other remotely stored files. The disagreement is presently the subject of a petition for certiorari before the United States Supreme Court seeking review of a decision from the Supreme Court of South Carolina. *See Jennings v. Jennings*, 736 S.E.2d 242 (S.C. 2012).[8]

Problem 4: The Statute Fails to Satisfy the Required Constitutional Standard

The fourth problem is the Fourth Amendment – or, more specifically, the statute's failure to measure up to constitutional standards. Existing lower court caselaw indicates that the provisions of 18 U.S.C. § 2703(b) fail to satisfy constitutional standards because they allow the government to obtain access to the contents of communications with less protection than a warrant based on probable cause. The leading case is *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), a Sixth Circuit decision involving government access to e-mails held by Yahoo!. Investigators relied on 2703(b) to subpoena Yahoo! for the contents of stored e-mails relating to a criminal enterprise. Yahoo! complied, and it gave investigators copies of thousands of e-mail messages without a warrant. The Sixth Circuit held that obtaining the contents of e-mails without a warrant was unconstitutional because users have a reasonable expectation of privacy in their e-mails just like their letters and phone calls. As a result, the provision of the SCA permitting the government to obtain e-mails with less process than a warrant did not satisfy the required Fourth Amendment standard. *See id.* at 288 ("[T]o the extent that the SCA purports to permit the government to obtain such emails warrantlessly, [that portion of] the SCA is unconstitutional.").

A number of courts have agreed with the Sixth Circuit since *Warshak*, including federal courts in Kansas[9] and the District of Columbia,[10] and the state of Washington Court of

[8] The Petition for Certiorari, Brief in Opposition, and an amicus brief filed before the United States Supreme Court are available at http://www.scotusblog.com/case-files/cases/jennings-v-broome/.

[9] In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917 at *5 (D.Kan. 2012) ("The Court finds the rationale set forth in *Warshak* persuasive and therefore

Appeals.[11] Other courts have applied *Warshak* to find a reasonable expectation of privacy in stored Facebook messages,[12] text messages,[13] faxes,[14] and password-protected websites.[15] The case law is not entirely settled, to be sure. Only one federal court of appeals has squarely addressed the issue. But the trend in the case law is to recognize fairly broad Fourth Amendment protection, backed by a warrant requirement, for stored contents such as e-mails.

Further, in my view *Warshak* is correct. Government access to remotely stored contents generally requires a warrant, meaning that the standards of § 2703(b) do not satisfy the constitutional floor provided by the Fourth Amendment. *See generally* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1017-31 (2010).

Problem 5: Disclosure to Law Enforcement Allows All Disclosure Without Limits

The fifth problem with the current statute is that permitted disclosure comes without limits. When a provider must disclose the contents of communications, there are no limits on how many contents it can disclose or what the government can do with the contents it receives. Recall that a typical Gmail user stores more than 17,000 e-mails in his account at any given time.[16] If the government obtains a subpoena or even a warrant requiring a provider to disclose contents in a suspect's account, current law contains no limits on what gets disclosed or used. The provider will send the government the entire contents of the

---

holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received thorough an electronic communications service provider.")

[10] United States v. Ali 870 F.Supp.2d 10 (D.D.C. 2012)

[11] State v. Hinton, 280 P.3d 476, 483(Wash.App. Div. 2 2012) ("While *Warshak* does not aid Hinton, its comparison of e-mails with traditional forms of communication is helpful and we adopt it to hold that text messages deserve privacy protection similar to that provided for letters.")

[12] R.S. ex rel. S.S. v. Minnewaska Area School Dist. No. 2149 --- F.Supp.2d ----, 2012 WL 3870868 at 12 (D.Minn. 2012).

[13] State v. Hinton, 280 P.3d 476, 483(Wash.App. Div. 2 2012) ("While Warshak does not aid Hinton, its comparison of e-mails with traditional forms of communication is helpful and we adopt it to hold that text messages deserve privacy protection similar to that provided for letters.")

[14] In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917 at *5 (D.Kan. 2012)

[15] United States v. D'Andrea, 497 F. Supp.2d 117, 121 (D. Mass. 2007).

[16] *See* Mike Barton, *How Much Is Your Gmail Account Worth?*, Wired, available at http://www.wired.com/insights/2012/07/gmail-account-worth/

account. The government then has access to all of those contents. Investigators can scan through all of the contents of a person's digital life without limit.

To phrase this problem in legal jargon, the existing statutory provisions contain no requirement of particularity, minimization, or non-disclosure. Particularity requires the government to specify which records it is seeking. Minimization requires the government to set up a filtering system: One person can go through the records and pass on the pertinent communications to investigators. And non-disclosure rules limit what the government can do with communications it has obtained. The current statute contains no such limits. That absence may be explained by the statute's relatively ancient origin. In 1986, few remotely stored records were kept. But today it is common for computer users to store tens of thousands of records of their daily life online. Remote storage has become cheap, allowing users to store everything.

As a result, government access to stored records raises a needle-in-a-haystack problem. The current statute allows the providers to simply hand over the entire haystack to investigators. Investigators can then look through the haystack at their leisure without limits and can use or disclose whatever they find regardless of its relevance to the investigation. Given the highly sensitive information commonly found in a personal e-mail account, the statute should take more care to protect the non-pertinent communications that ordinarily will make up the bulk of the contents of communications found in an e-mail account. The Fourth Amendment may already impose some of these limits, and statutory authorities from the Wiretap Act adopt other limits when the government obtains a wiretap order.[17] The same protections should be written into the provisions for lawful access to stored content.

——

Thank you for the opportunity to testify. I look forward to your questions.

[17] *See, e.g.*, In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917 (D. Kan. 2012) (imposing particularity requirements on a warrant for the contents of an e-mail account under the Fourth Amendment); *See* United States v. McGuire, 307 F.3d 1192 (9th Cir. 2002) (discussing minimization requirements for electronic communications under the Wiretap Act).