United States 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, DC
September 23, 2010

Statement of Fred H. Cate
Distinguished Professor and C. Ben Dutton Professor of Law
Director, Center for Applied Cybersecurity Research
Indiana University

Chairman Nadler, Representative Sensenbrenner, and Members of the Subcommittee,

My name is Fred Cate, and I am a Distinguished Professor and C. Ben Dutton Professor of Law at the Indiana University Maurer School of Law, and the director of Indiana University's Center for Applied Cybersecurity Research, a National Center of Academic Excellence in Information Assurance Education and in Information Assurance Research.

For the past 20 years I have had the privilege of researching and teaching about a variety of privacy, security, and other information law and policy issues. I served as a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information, and counsel to the Department of Defense Technology and Privacy Advisory Committee.

In addition to my academic appointment, I am also a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, a member of Microsoft's Trustworthy Computing Academic Advisory Board, a member of Intel's Privacy and Security External Advisory Board, editor of the Privacy Department of the IEEE's (Institute of Electrical and Electronic Engineers) *Security & Privacy*, and one of the founding editors of the Oxford University Press journal, *International Data Privacy Law*, among other activities.

I am testifying today on my own behalf; the views I express should not be attributed to any organization with which I am affiliated.

Chairman Nadler, I want to begin by thanking for your leadership in holding this important series of hearings of Electronic Communications Privacy Act reform, and for inviting me to participate in today's hearing on Title II of that Act, the Stored Communications Act (SCA),[1] and how it affects, and is affected by, the rise of cloud computing.

[1] Pub. L. No. 99-508, Title II, § 201, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701-2711).

I have been asked to present a brief overview of the SCA and how it interacts with cloud computing, and I am delighted to do so. I will begin with a brief survey of the constitutional background to the statute.

The Fourth Amendment and the "Third Party" Doctrine

The primary constitutional limit on the government's ability to obtain personal information about individuals is the Fourth Amendment, which reflects the Framers' hostility to "general searches"—searches not based on specific suspicion.[2]

The Fourth Amendment does not purport to keep the government from conducting searches or seizing personal information. As interpreted by the Supreme Court, it requires that the government generally conduct searches with a warrant issued by a court.[3] For a court to issue a warrant, the government must show "probable cause" that a crime has been or is likely to be committed and that the information sought is germane to that crime.[4] The Supreme Court also generally requires that the government provide the subject of a search with contemporaneous notice of the search.[5]

The Court has repeatedly found that the Fourth Amendment (and its requirement for a warrant) only apply to searches of material or places in which there is a "reasonable expectation of privacy." In his 1967 concurrence in *Katz v. United States*, Justice Harlan wrote that reasonableness was defined by both the individual's "actual," subjective expectation of privacy and by an objective expectation that was "one that society was prepared to recognize as 'reasonable.'"[6] The Court adopted that test for determining what was "private" within the meaning of the Fourth Amendment in 1968 and continues to apply it today.[7]

The Court wrote in *Katz* that "what a person knowingly exposes to the public . . . is not the subject of Fourth Amendment protection."[8] While in the context in which this was originally used, this language is perfectly understandable, the Court's subsequent interpretations of this passage have created a significant exception to the Fourth Amendment's scope and protection.

The Supreme Court applied this language in 1976 in *United States v. Miller*[9] to hold that there can be no reasonable expectation of privacy in information held by a third party. The case involved cancelled checks, to which, the Court noted, "respondent can assert neither ownership nor possession."[10] Such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business,"[11] and therefore the Court found that the Fourth Amendment is not implicated when the government sought access to them:

---

[2] U.S. Constitution amend. IV.
[3] Akihl Reed Amar, *The Constitution and Criminal Procedure* 3-4 (1997).
[4] 68 *American Jurisprudence 2d*, Searches and Seizures § 166 (1993).
[5] Richards v. Wisconsin, 520 U.S. 385 (1997).
[6] 389 U.S. 347, 361 (1967).
[7] Terry v. Ohio, 392 U.S. 1 (1968).
[8] 389 U.S. at 351-52.
[9] United States v. Miller, 425 U.S. 435 (1976).
[10] Id. at 440.
[11] Id. at 442.

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[12]

The Court's decision in *Miller* is remarkably sweeping. The bank did not just happen to be holding the records the government sought. Instead, the Bank Secrecy Act required (and continues to require) banks to maintain a copy of every customer check and deposit for six years or longer.[13] The government thus compelled the bank to store the information, and then sought the information from the bank on the basis that since the bank held the data, there could not be any reasonable expectation of privacy and the Fourth Amendment therefore did not apply.[14] A majority of the Supreme Court was not troubled by this application of the Fourth Amendment.[15]

The Court reinforced its holding in *Miller* in the 1979 case of *Smith v. Maryland*, involving information about (as opposed to the content of) telephone calls.[16] The Supreme Court found that the Fourth Amendment is inapplicable to telecommunications "attributes" (e.g., the number dialed, the time the call was placed, the duration of the call, etc.)—what today we would describe as "metadata"—because that information is necessarily conveyed to, or observable by, third parties involved in connecting the call.[17] "[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[18]

Under the Supreme Court's "third party doctrine," records disclosed to, and held by, third parties receive no constitutional protection. Searches of these records need not be reasonable. And no judicial oversight is involved.

The Stored Communications Act

Congress responded to the Court's decisions with a variety of laws, including the Right to Financial Privacy Act,[19] which deals with access to financial records, and the Pen Register Act,[20] which deals with access to telephone calling records. Congress also enacted the Stored Communications Act—

[12] Id. at 443 (citation omitted).

[13] 12 U.S.C. § 1829b(d); see 425 U.S. at 436; California Bankers Assn. v. Shultz, 416 U.S. 21 (1974).

[14] 425 U.S. at 443.

[15] Id. at 444 ("even if the banks could be said to have been acting solely as Government agents in transcribing the necessary information and complying without protest with the requirements of the subpoenas, there would be no intrusion upon the depositors' Fourth Amendment rights").

[16] 442 U.S. 735 (1979).

[17] Id. at 743.

[18] Id.

[19] 12 U.S.C. §§ 3401-3422.

[20] 18 U.S.C. §§ 3121-3127.

Title II of ECPA and the subject of today's hearing—which deals with communications and other records in electronic storage, such as e-mail and voice mail.[21]

The 1986 report on the SCA explains that computer users at that time generally used network services in two ways. First, they used network services to send and receive email. Second, they used those services to remotely store and process data.[22] Both services raised privacy concerns because both involve third parties maintaining copies of individual users' mail, documents, and other records. Under the Supreme Court's third-party doctrine, these materials would receive no Fourth Amendment protection.

The SCA divides stored electronic communications into two categories, reflecting the two predominate uses in 1986. An "Electronic Communication Service" ("ECS") is defined by the statute as the "temporary, intermediate storage of a wire or electronic communications incidental to the electronic transmission thereof" and storage for "backup protection."[23] A "Remote Computing Service" ("RCS") is the "provision to the public of computer storage or processing services by means of an electronic communications system."[24]

Records within an ECS are further divided into subcategories based on duration of storage. Government demands for records held as part of an ECS and that had been stored for 180 days or less require a traditional warrant issued by a competent court.[25] To obtain material within an ECS that has been stored for more than 180 days, or to obtain material stored as part of an RCS, the government has three options: it can use a warrant, it can use a subpoena (an administrative subpoena, a grand jury subpoena, or a trial subpoena), or it can use a court order based on "specific and articulable facts" (sometimes called a "2703(d) order" or a "d order").[26] If the government does not provide notice to the individual, then a warrant is required.[27] If it does provide contemporaneous or, in some cases, delayed notice, then a subpoena or 2703(d) order may be used.[28] Under either category, a service provider may *voluntarily* provide the records to the government (subject to certain limitations).[29]

Complicating this analysis is the fact that the Department of Justice believes, and most courts to consider the issue have agreed, that the warrant requirement for records stored 180 days or less only applies to *unopened* email or other communications content.[30] Under this view, once email has been

---

[21] Pub. L. No. 99-508, Title II, § 201, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701-2711).

[22] S. Rep. No. 99-541, at 2-3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3556-57.

[23] 18 U.S.C. § 2510(17).

[24] Id. at § 2510(17)(B).

[25] Id. at § 2703(a). See generally Daniel J. Solove, "Electronic Surveillance Law," 72 *George Washington Law Review* 1264, 1283 (2004).

[26] 18 U.S.C. at §§ 2703 (a)-(b).

[27] Id. at § 2703(b)(1)(A).

[28] Id.

[29] Id. § 2702. These are carefully analyzed in Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 *George Washington Law Review* 1208 (2004).

[30] See Kerr, supra at nn.82-95 and sources cited therein.

opened, the government may access it from an ECS provider under the lower standard applicable to RCS material. The Ninth Circuit has taken a different view.[31]

information *about* a customer's account, or about communications (but not including the communications content), maintained by a communications provider can be obtained by the government by providing a warrant, a 2703(d) order, or, in the case of telemarketing fraud, upon formal written request.[32] Other "basic subscriber information," including name, address, length of service and types of service, means of payment, and local and long distance connection records, can be obtained with an administrative subpoena, a grand jury subpoena, or a trial subpoena.[33]

The following table summarizes the type of authorization necessary to obtain personal information held by an ECS or RCS provider under the SCA.

Stored Communications Act Summary of Authorization Necessary to Obtain Data			
ECS contents held unopened in "temporary, intermediate storage" or stored for "backup protection" for 180 days or less	ECS contents after they have been opened, or held unopened in "temporary, intermediate storage" or stored for "backup protection" for more than 180 days, or RCS contents	Information about a subscriber account (but no contents of records)	"Basic subscriber information" (but no contents of records)
Search warrant	If no notice: search warrant; if notice: a subpoena or a 2703(d) order	2703(d) order or, in the case of telemarketing fraud, formal written request	A subpoena

Violations of the SCA carry a minimum fine of $1,000; no exclusionary rule applies.[34]

Critique

The SCA has been the subject of considerable criticism. That criticism generally might be divided into five broad categories. The first is that the statute is "dense and confusing."[35] Law enforcement officials, service providers, and courts have considerable difficulty understanding and applying the statute. The result is that it is often misapplied. This situation serves no one's interest, because it means that the SCA provides inadequate protection for privacy and inadequate certainty for when law enforcement can access important information.

The second category of criticism is that the SCA is ambiguous, especially in the light of significant changes in online services markets. It is not clear that the market ever divided neatly into

[31] In *Theofel v. Farey-Jones*, 359 F.3d 1066, 1076 (9th Cir. 2004), the Ninth Circuit concluded that all e-mails held by a server are protected under the ECS rules until "the underlying message has expired in the normal course," regardless of whether the e-mail has been accessed.

[32] 18 U.S.C. § 2703(c)(1).

[33] Id. § 2703(c)(2).

[34] See Daniel J. Solove, "Electronic Surveillance Law," 72 *George Washington Law Review* 1264, 1284 (2004).

[35] See Kerr, supra.

communications services and remote storage and processing services, but today, with the advent of a massive digital economy, those lines are infinitely more difficult to draw. Similarly, the content versus noncontent information distinction, which might have made sense with physical mail (contents vs. envelope) or even telephone calls (content vs. number dialed), is much harder to apply with digital materials. And even the distinction between voluntary disclosure and law enforcement demands has proved problematic in practice. For example, which is it when a state attorney general contacts an ISP and asks for its "voluntary" assistance identifying child pornography, promising to laud the business if it helps and excoriate it in the press if it does not?

The third category of criticism concerns the lack of publicly available, aggregate statistics detailing the extent to which third party providers are routinely compelled to deliver their customers' communications and other private data to law enforcement agencies. Congress already requires mandatory annual reports for the use of wiretap, pen register, and trap and trace orders. As a result, academics, public interest advocates, and policy makers are generally able to determine the extent to which such surveillance methods are used.[36] Congress has not created similar statutory reporting requirements for law enforcement agencies' use of warrants, "27303(d) orders, and subpoenas to obtain individuals' communications contents and other private data. The only information about the scale of such activities available to policy makers comes from voluntary disclosures by a few service providers willing to discuss such practices.[37] Because most service providers do not disclose this information, Congress and the people have no reliable data to determine the scale of this form of electronic surveillance, which is likely to outnumber the 2,376 wiretap orders granted in 2009, and the 11,126 pen registers and 9,773 trap and trace orders granted in 2008.[38]

The fourth category of criticism concerns the level of protection provided by the SCA as a legal matter. Under the third-party doctrine, the Supreme Court has determined that material in the hands of third parties gets no constitutional protection. In a series of statutes, Congress has clearly indicated that it disagrees. However, the SCA provides quite limited protection for most of the material to which it applies, requiring only a subpoena if contemporaneous notice is given to the affected individual(s). Subpoenas require no judicial oversight; many agencies issue them on their own authority, and prosecutors often issue subpoenas in the name of grand juries without any procedural determination that the information sought is relevant. Moreover, subpoenas do not have to target information about specific individuals; a law enforcement agency could use a subpoena to demand all of the records held by a provider of ECS or RCS. Finally, the SCA does not apply to all data stored in the hands of a third party, or even all data stored electronically in the hands of a third party. ECS and RCS have specific definitions in the statute, and those definitions exclude the significant range of internet sites that provide neither communications services nor remote processing services. As a result, even in 1986, it was an inadequate response to the Court's third-party doctrine.

---

[36] 18 U.S.C. § 2519. See generally, Wiretap Reports, Administrative Office of the US Courts, available at: http://www.uscourts.gov/Statistics/WiretapReports.aspx.

18 U.S.C. § 3126. These reports are not made public, but have been obtained by researchers via the Freedom of Information Act. The reports for the years 1999-2008 can be found at http://www.spyingstats.com/.

[37] For example, see Google's government request tool, available at: http://www.google.com/governmentrequests/.

[38] The pen register reports for 2009 have not yet been obtained by privacy advocates. 2008's report can be found here: http://files.spyingstats.com/pr-tt/DOJ-pen-registers-2004-2008.pdf

The fifth and final category focuses on the extent to which dramatic changes in technologies and online services—especially cloud computing—have rendered both the third-party doctrine and the SCA inadequate to protect privacy today. Professor Daniel Solove has written: "We are becoming a society of records, and these records are not held by us, *but by third parties*."[39] These records are generated through our daily transactions, our searches online, and our internet browsing, but they are also the result of a growing number of online services that provide free storage as a way of attracting customers (and viewers for online advertising). Remote storage is wide available today for financial records, test results from home health devices, photographs, music, data about collections (of books, music, or hobbies), remote computer back-up, and email. Remote storage facilitates off-site back-up and can make data more accessible from different locations.[40]

To take just one practical example, and one of the types of material the SCA was intended to protect, in 1986 email was just coming into widespread use. The norm was for email to be retrieved and stored locally, on the user's machine, because storage was expensive and few vendors wished to provide it. As the price of storage has dropped, and competition in online services has grown, most email service providers now offer vast amounts of email storage—in fact, some now offer *unlimited* storage—as a way to attract customers. Remote storage of email is today a fact of life and a basic consumer expectation. It facilitates ease of access as we move from one computing device to another—so I can access the same email from my office desktop, my laptop, my iPhone, and my home computer; it allows for automatic backup; and it makes it easier to share photos, music, and movies, which is a growing use of email. Moreover, as the price of storage has dropped and processing power and search capabilities have grown, more people are now keeping all of their email as a virtual filing system. Under the framework of which the SCA is a part, email gets one standard of protection while being composed and later retained in their "sent" mail folder, one while in transit, one in remote storage until opened or 180 days has passed, and one standard after being opened or 180 days has passed.[41] Most of the standards of protection provided by the SCA (all of the standards applicable to remove storage for communications or as part of a remote processing service) are substantially weaker than that ordinarily required by the Fourth Amendment, and do not even require judicial oversight. And even these weaker standards of protection do not apply where no communications service or remote processing is involved.

This is inadequate protection: inadequate to protect privacy and inadequate to provide government officials with clarity about what they are permitted by law to access and the procedures they must follow when they do so. The officials run the risk of either moving forward too aggressively, and thereby trampling civil rights and potentially exposing themselves to liability, or holding back through an excess of caution and thus failing to serve national interests effectively. These are not speculative costs; they are well documented in other legal settings in numerous Inspector General and other government reports.[42]

---

[39] Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 *Southern California Law Review* 1083, 1089 (2002) (emphasis added).

[40] See generally Fred H. Cate, "Government Data Mining: The Need for a Legal Framework," 43 *Harvard Civil Rights-Civil Liberties Law Review* 436 (2008).

[41] See generally James X. Dempsey, "Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology," *Ninth Annual Institute on Privacy and Security Law* (PLI) 543, 562 (2008).

[42] See *Semiannual Report to Congress [on the] Federal Bureau of Investigation, October 1, 2007-March 31, 2008*, supra; *A Review of the FBI's Use of National Security Letters* (2008), supra; *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006* (2008), supra; *The FBI's Use of National Security Letters and Section 215 Requests for Business Records*, supra (statement of Glenn A. Fine);.*A Review of the Federal Bureau of*

Moreover, as consumers embrace ever more complex information technologies, such as GPS enhanced mobile devices and cloud computing services, it becomes less likely that average users understands the technologies on which they depend, and the degree to which their private data is transmitted to third parties. Therefore, the concept of "voluntary disclosure" on which the third-party doctrine depends, and which is reflected in the considerably lower protection that the SCA accords to such information, is simply not warranted. Earlier this month the Third Circuit ruled on this very issue, in a case involving the application of the SCA to stored location data, deciding that:

> A cell phone customer has not "voluntarily"' shared his location information with a cellular provider in any meaningful way . . . [because] it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information."[43]

Conclusion

There seems unanimous agreement that the SCA needs to be revised. The Digital Due Process Coalition has put forth one set of proposals that command broad industry and academic support, and are specifically designed to provide substantive protection for privacy, while also permitting law enforcement access to relevant documents, and to do so in a way that is clear and easy to understand.[44] As a member of that coalition, I hope you will give those proposals your careful consideration.

As you think about ways forward, I encourage you to remember that none of the protections under the Fourth Amendment, in the current SCA, or in the Digital Due Process Coalition's proposals block access to relevant records or the ability for providers to voluntarily provide law enforcement agencies with such information in emergencies. Rather, the goal is to ensure that an appropriate process is followed and that such a process includes appropriate oversight.

Thank you again for the opportunity to participate today.

Investigation's Use of National Security Letters (2007), supra; *FBI Use of National Security Letters*, supra (statement of Glenn A. Fine); *The FBI's Use of National Security Letters and Section 215 Requests for Business Records*, supra (statement of Glenn A. Fine).

[43] In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, No. 08-4227 (3d Cir., Sep. 4, 2010), available at http://www.ca3.uscourts.gov/opinarch/084227p.pdf.

[44] See http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

Biography

Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, Adjunct Professor of Informatics and Computing, and director of the Center for Applied Cybersecurity Research at Indiana University. He works at the forefront of privacy, security, and other information law and policy issues.

He is a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, a member of Microsoft's Trustworthy Computing Academic Advisory Board, Intel's Privacy and Security External Advisory Board, the Board of Directors of the Center for Applied Identity Management Research, the Board of Directors of The Privacy Projects, the Board of Advisors of Trustee, and BNA's *Privacy & Security Law Report* Advisory Board. He serves as the Privacy Editor for the IEEE's (Institute of Electrical and Electronic Engineers) *Security & Privacy* and is one of the founding editors of the Oxford University Press journal, *International Data Privacy Law*. He participates in privacy reviews of classified programs in the Department of Homeland Security and holds a TS-SCI clearance.

Previously, Professor Cate served as a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention, reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information, counsel to the Department of Defense Technology and Privacy Advisory Committee, reporter for the third report of the Markle Task Force on National Security in the Information Age, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, and chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities.

Professor Cate has testified before numerous congressional committees, and he speaks frequently before professional, industry, and government groups. He has spoken throughout the United States and in Belgium, Canada, China, Finland, France, Germany, Italy, Japan, Switzerland, Taiwan, Trinidad & Tobago, and the United Kingdom. He is the author of more than 100 articles and books, including *Privacy in the Information Age, The Internet and the First Amendment*, and *Privacy in Perspective*. He appears regularly in national media.

Professor Cate is the President and a Fellow of the Phi Beta Kappa Society and an elected member of the American Law Institute. He attended Oxford University and received his J.D. and his A.B. with Honors and Distinction from Stanford University. He is listed in *Who's Who in the World*, *Who's Who in America, Who's Who in American Law*, and *Who's Who in American Education*. *Computerworld* included him in its two most recent rankings of "Best Privacy Advisers."