Testimony of Cameron F. Kerry
General Counsel
United States Department of Commerce

Before the
Committee on the Judiciary
United States Senate

"The Electronic Communications Privacy Act:
Government Perspectives on Protecting Privacy in the Digital Age"

April 6, 2011

I. Introduction.

Chairman Leahy, Ranking Member Grassley, and Members of the Committee, thank you for the opportunity to testify on behalf of the Commerce Department to discuss updating the Electronic Communications Privacy Act of 1986 (ECPA). I am pleased to again appear before you with the Department of Justice.

The Administration fully understands the Committee's rationale for reexamining ECPA. In the twenty-five years since ECPA was enacted, there has been a revolution in how Americans communicate and in how they transmit, manipulate, and store records and information. As this Committee wisely stressed in 1986, privacy protections "must advance with technology" or privacy will "gradually erode as technology advances."[1] Indeed, the rapidly changing technological environment raises not only privacy and civil liberties issues -- it also presents challenges for law enforcement and national security personnel as they seek to prevent terrorism, espionage, and other criminal and malicious acts from being committed online and in the electronic world. To ensure that ECPA continues to accommodate privacy, civil liberties, innovation, the needs of law enforcement and national security, and other important interests, the law must not remain static as technology, business practices, and consumer behavior change.

[1] S. Rep. No. 99-541, at 5, reprinted in 1986 U.S.C.C.A.N. 3555, 3559.

Since Mr. Baker and I testified before this Committee last September, the Department of Commerce and the Department of Justice have been working together to develop a specific set of legislative proposals to share with you. We have not completed this process, but we continue to discuss options for possible ECPA amendments.

II. Private Sector Stakeholders' Perspectives on Our Current ECPA Framework.

The Internet-based digital economy has sparked tremendous innovation. During the past fifteen years, networked information technologies – personal computers, mobile phones, wireless connections and other devices – have transformed our social, political, and economic landscape. A decade ago, going online meant accessing the Internet on a computer in your home, most often over a copper-wire telephone line. Today, "going online" also includes smartphones, tablets, portable games, and interactive TVs, with numerous companies developing global computing platforms in the "cloud."

These powerful and exciting developments also raise new privacy and civil liberties issues and new challenges for law enforcement. For this reason, the Commerce Department's Internet Policy Task Force has been charged with identifying and developing a privacy framework for Internet-based communications that meets the needs of the 21st century information economy. On April 23, 2010, we released a Notice of Inquiry on "Information Privacy and Innovation in the Internet Economy," which prompted more than seventy comments. Although this Notice of Inquiry did not mention ECPA, multiple commenters highlighted a critical need to reexamine the statute.[2] Those comments, as well as information gathered in various listening sessions, called attention to the impact of technological changes on ECPA.

---

[2] *See, e.g.*, Google Comments, at 4, in *Request for Reply Comments on Information Privacy and Innovation in the Internet Economy*, Docket No. 101214614-0614-01 (filed Jan. 28, 2011), *available at* http://www.ntia.doc.gov/comments/101214614-0614-

On December 16, 2010, the Commerce Department published ECPA findings (among other proposals) in a report entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Privacy Framework" (a copy of which is attached for the record). Our report contained the following recommendation:

> The Administration should review the Electronic Communications Privacy Act, with a view to addressing privacy protection in cloud computing and location-based services. A goal of this effort should be to ensure that, as technology and market conditions change, ECPA continues to appropriately protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.

In response to this recommendation, the Commerce Department received further written comments from industry and consumer groups. All comments endorsed updating ECPA.[3]

01/attachments/FINALCommentsonDepartmentofCommercePrivacyGreenPaper%20(3).pdf (Google Comments). For convenience, all subsequent citations to "Comments" or "Reply Comments" refer to pleadings submitted on January 28, 2011, in Docket No. 101214614-0614-01. *See also* Microsoft Comments, at 10-11, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/Microsoft%20Comments%20on%20Commerce%20Privacy%20Green%20Paper%20-%20final.pdf; Digital Due Process Coalition Comments , at 26-27 (filed June 14, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Digital%20Due%20Process%20Coalition%20Comments.pdf (DDPC Comments); Comments of AT&T, Inc., at 34-35, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/ACF320.pdf (AT&T Comments); Comments of the American Civil Liberties Union Comments, at 10-11, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/Final%20Commerce%20Comments%20January%202011%20on%20DNT.pdf (ACLU Comments); Center for Democracy and Technology, at 5-6, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/CDT%20privacy%20comments.pdf; (CDT Comments); Computer and Communications Industry Association Comments, at 4-7, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/CCIA%20Commerce%20Comments.pdf (CCIA Comments); Deirdre K. Mulligan Comments, at 3 (June 14, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Deirdre%20K%2E%20Mulligan%20Comments%2Epdf (Mulligan Comments); Information Technology and Innovation Foundation, at 6 (June 14, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ITIF%20Comments%2Epdf.

[3] In response to the Commerce report's ECPA recommendation, supportive comments were submitted by eBay, Inc., Net Choice, Privacy Rights Clearinghouse, AT&T, Verizon, ACLU, General Electric, Microsoft, Google, Electronic Frontier Foundation, World Wide Web Consortium, and the Computer & Communications Industry Association, among others. All comments are available here: http://www.ntia.doc.gov/comments/101214614-0614-01/. In addition, the following companies and consumer groups have publically called for simplifying, clarifying, and unifying the ECPA standards, in response to changes in technology and new services and usage patterns: AOL, Amazon, Data Foundry, Facebook, Hewlett-Packard, Intel, Intuit, Qwest, Salesforce.com, American Library

Commenters drew attention to privacy issues surrounding new technologies, noting that the laws permitting government access to Internet communications (and records associated with customer accounts) under certain conditions prompt consumer concerns about the privacy and security of their online personal data. Commenters also stressed that "[c]ompliance with ECPA's requirements should not depend on the nature of the technology, but rather on the nature of the information sought and on Congressional determinations about consumers' reasonable expectations of privacy."[4] AT&T pointed out that ECPA's provisions have been interpreted inconsistently, raising the specter of liability and the possibility that a vast amount of personal information generated by today's digital communications services may not be protected in the same ways as comparable information in other forms.[5]

Commenters also reminded us of the social importance and economic value of recent digital communications innovation and new types of information, such as geolocation data collected from cell phones and content (text, voice, and video) stored online and accessible from anywhere on the Internet. These technologies allow companies tremendous flexibility in how they manage and store data, relate to customers, and assemble their workforces. They also provide new avenues for everything from forming friendships to organizing for political advocacy. As the Committee heard from the private sector panel on this issue last September,

---

Association, Americans for Tax Reform, Citizens Against Government Waste, Consumer Action, Future of Privacy Forum, NetCoalition, Software and Information Industry Association, TechAmerica, TechFreedom, and the Telecommunications Industry Association.

[4] Comment of Verizon and Verizon Wireless, at 14, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/01%2028%2011%20Verizon,%20Verizon%20Wireless%20Comments%20NTIA%20Privacy%20NOI.pdf. *See also* Mulligan Comments, *supra* note 2, at 3

[5] AT&T Comments, *supra* note 2, at 34 ("It is reasonable to conclude that law enforcement and private sector actors, such as ISPs and other service providers in the telecommunications and technology sectors, would benefit from specific guidance on how, to what extent, and by what means law enforcement may properly request and obtain access to the data collected incidental to the services that are provided.").

uncertainty about how ECPA applies to these types of data may hinder the adoption of new technologies by individuals and businesses and may impede innovation.[6]

The revolution in how Americans communicate and how they transmit, manage, and store information continues at an accelerating pace. Internet traffic in the United States alone approaches three petabytes per month (that is a three followed by fifteen zeros), and is growing by 40 - 50 percent annually.[7] This astonishing flow of traffic reflects how the Internet has become the communications medium of choice for most Americans, especially younger Americans. Increasingly, emails, mobile text messages, and documents stored and shared online are replacing letters, phone calls, and desktop computing. The traffic includes not only email messages, but also friend updates, photo comments and tags, and status changes; storage involves photos and videos, as well as emails and documents. Moreover, as one commenter pointed out, as Internet usage intensifies, Americans leave a myriad of "traceable trails online – the websites we've visited, the search terms we've used."[8]

III. ECPA Should Reflect Changes in Technology and Consumer Uses and the Needs of Law Enforcement and National Security.

At September's hearing, Mr. Baker and I agreed that these changes in technology, businesses practices, and consumer habits and expectations naturally raise the question whether changes in ECPA are needed to ensure that the balance originally struck in 1986 between privacy, law enforcement, and national security needs remains fair and appropriate today.

---

[6] *See The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 111th Cong., 2d Sess., at 4 (2010) (statement of Brad Smith, General Counsel, Microsoft Corporation), *available at* http://judiciary.senate.gov/pdf/10-09-22SmithTestimony.pdf; *id*., at 14 (Statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology), *available at* http://judiciary.senate.gov/pdf/10-09-22DempseyTestimony.pdf. *See also* Comments of AT&T, *supra* note 5, at 34 (noting that "heightened uncertainty may stifle innovation").

[7] University of Minnesota, "Minnesota Internet Traffic Studies," *available at* http://www.dtc.umn.edu/mints/.

[8] Reply Comments of NetChoice, at 19, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/NetChoice%20Comments%20on%20Commerce%20Green%20Paper%20FINAL.pdf.

Today, the Administration supports the Committee's decision to consider this question and looks forward to engaging with you and other Members of Congress in the task.

ECPA itself embodies Congress's recognition that the law must adjust as technology advances. When Congress enacted the landmark Wiretap Act in 1968, it specifically excluded transmission of data from that statute's protection against interception. In 1986, Congress extended these protections to data transmissions because "[i]n the intervening years, data transmission and computer systems have become a pervasive part of the business and home environment."[9] As Mr. Baker pointed out in September, Congress substantially amended ECPA twice since 1986 to ensure that its provisions "evolved to account for changing times."[10]

There is another reason why your ongoing reexamination of ECPA is timely. In recent years, a number of courts have struggled to apply the law to a rapidly changing communications environment. One result has been several decisions that create uncertainty and confusion for consumers, law enforcement, the business community, and the Nation's innovators. I would like to discuss two recent cases.

The first case, a September 2010 decision by the U.S. Court of Appeals for the Third Circuit, concerns the procedures and standards by which law enforcement agencies may obtain certain cell location information.[11] There have been a series of decisions from district courts and magistrates on this issue, without any consensus about what the law including section 2703(d) of ECPA requires. The Third Circuit was the first appellate court to consider the question. It concluded that a court may refuse to issue an order pursuant to section 2703(d) to enable the

---

[9] H. Rep. No. 99-647, at 21, 99th Cong., 2d Sess. (1986).
[10] *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 111th Cong., 2d Sess., at 6 (2010) (statement of James A. Baker, Associate Deputy Attorney General, United States Department of Justice), *available at* http://judiciary.senate.gov/pdf/10-09-22BakerTestimony.pdf.
[11] *Application of the United States*, 620 F.3d 304 (3d Cir. 2010).

government to obtain cell location information, even if the government satisfies the legal standard set forth in that section.[12] At the same time, the Third Circuit articulated no clear standards to guide lower courts' exercise of the discretion it accorded them.[13] Congress should examine ECPA's standards and procedures concerning government access to such information, and ensure that principled reasons continue to support those standards and procedures.

The second case is *United States v. Warshak,* a December 2010 decision in which the U.S. Court of Appeals for the Sixth Circuit held that, under certain circumstances, an individual has a Fourth Amendment-protected privacy interest in private emails, even when those emails are in the possession of a third-party. The court reasoned that "[a]s some forms of communications begin to diminish, the Fourth Amendment must recognize and protect nascent ones as they arise."[14] The Sixth Circuit wrote that email "plays an indispensible part in the Information Age," and it "requires strong protection under the Fourth Amendment . . ."[15]

The *Warshak* court also relied in part on the Supreme Court's June 2010 decision in *City of Ontario v. Quon*,[16] which considered the reasonableness, under the Fourth Amendment, of the city's audit of text messages that Quon transmitted via a city-provided communications service. In considering whether Quon had a reasonable expectation of privacy in those messages, the Court acknowledged that "cell phones and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."[17] It also noted, however, that "employees who need cell

---

[12] *Id*. at 315-316.
[13] *Id*. at 316-319.
[14] *United States v. Warshak*, 631 F.3d at 284, 286.
[15] *Id*. at 286.
[16] *Id*. at 286 (quoting *Quon*, 130 S.Ct. 2619, 2630, 2631 (2010)).
[17] *Quon*, 130 S.Ct. at 2630.

phones or similar devices for personal matters can purchase and pay for their own."[18] Ultimately, the Court did not resolve the privacy issue; instead, the Court assumed without deciding that Quon had a reasonable privacy interest in text messages conveyed over the city-provided communications service.[19] It nevertheless held that the city's audit of those messages was reasonable because, among other things, the audit of "Quon's employer-provided pager was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his phone line, would have been."[20]

Warshak is the law only in the Sixth Circuit, and the U.S. government is determining whether to seek Supreme Court review. Until such time as the Court squarely addresses the issue, the law as to what protection the Fourth Amendment affords to the messages and other customer content transmitted and stored electronically will be unsettled, and the resulting uncertainty will create challenges for consumers, businesses, and law enforcement. As Congress reassesses ECPA, one clear goal should be establishing clear and consistent rules in the area for the new communications marketplace.

The Internet offers users the ability to store and access information content anywhere across the Web (what ECPA called 'remote computing') with equal ease as was traditionally done on a user's local computer. An important subject for legislative consideration is whether there should be identical statutory protections regardless of whether a user stores information on a provider's computer or locally in the user's own computer.

In determining whether to modify ECPA's current framework with respect to customer content, Congress should be guided by two overarching considerations. First, there should be a

---

[18] *Id.*
[19] *Id.*
[20] *Id.* at 2631.

principled relationship between the legal protections and procedures that apply to law enforcement access to electronic information (including both content and customer identification and transactional information) and the legal protections and procedures for comparable materials in the physical world. What those legal protection and procedures are should be determined by reference to a number of factors, including the privacy expectations of the parties involved, who has access to or control of the information, and the reasonable needs of law enforcement and national security.

Second, the legal protection afforded to electronic content should not turn simply on factors that are disconnected from ordinary citizens' reasonable privacy interests. As Senator Cardin noted at September's hearing, one may question whether the so-called 180-day rule – the notion that privacy protection accorded to an electronic message should be different 180 days after it is sent from the protections that apply on day 181 – should continue to be the law. If Congress wants to revisit this issue, as in the physical world, the appropriate level of privacy protection for online information should flow from an assessment of other factors, including the expectation of privacy surrounding the mode of communication used in connection with the content, who has access and use of that information, and the interests of law enforcement and national security.

These considerations, of course, cannot by themselves define the appropriate legal protection for electronic content. Close questions remain on which reasonable minds can differ. The resolution of those questions will require Congress once again to strike a fair balance

between the competing interests, including privacy, the needs of law enforcements and national security, innovation, and international competitiveness.[21]

Applicable rules should also recognize the need of law enforcement and national security agencies' timely and effective access to content needed to enforce the law and to protect the public, especially in circumstances where such access is time-sensitive. The Fourth Amendment applies most clearly to materials in my home, including content stored on my home computer. If law enforcement agents wish to seize my computer from my home, without my consent or the consent of someone else with access to and control over my home, under most circumstances, they must first obtain a warrant. Alternatively, they could issue a subpoena commanding me to bring my computer to them. In either case, there are opportunities for a court to review, or for an affected individual to challenge, the sufficiency of law enforcement's basis for access. By contrast, one criticism of ECPA is that, although government must notify the targeted individual if it seeks content from a service provider subject to ECPA without a warrant, it can delay notice to the individual for a considerable period of time upon a demonstration that the notified individual is likely to destroy evidence, threaten witnesses, flee, or cause some other adverse result spelled out in the statute.[22] Any rule or procedure must accommodate exigent circumstances; there are conditions that justify not informing an individual in the midst of an

---

[21] *See* Baker Testimony, *supra* note 10, at 7; *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 111th Cong., 2d Sess., at 2 (2010) (statement of Cameron F. Kerry, General Counsel United States Department of Commerce), *available at* http://judiciary.senate.gov/pdf/10-09-22KerryTestimony.pdf.

[22] *See Warshak v. United States*, 490 F.3d 455, 468-469, 475 (6th Cir. 2007), *vacated, 532 F.3d 521 (6th Cir. 2008)* (government's attempt to seize emails from an ISP without a warrant was unlawful because defendant did not have adequate notice and an opportunity to challenge). In the *Warshak* litigation, the defendant was not aware that the government had seized some of his emails for more than a year after the seizure occurred. *See id*. at 460. *See also* Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," at 31 (2004), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860.

ongoing criminal or national security investigation, such as kidnappers, child molesters, or foreign spies.

IV. Conclusion.

Thank you again for inviting the Department of Commerce to testify on this important issue. As I stated last September, in establishing a clear and predictable privacy framework for electronic communications, ECPA contributed to the explosion in electronic communications that has produced enormous economic and social benefits for our nation over the last quarter century. Today, the communications revolution ECPA helped to fuel has produced new technologies, new services, new usage patterns, and new habits and expectations that require close examination of ECPA. The task is to determine whether additional changes are now needed to enhance privacy and to enable the government to carry out its law enforcement and national security responsibilities, so that in the future, as in the past, ECPA will provide a well-marked road map for providers, law enforcement, and citizens, and will enable further innovation and growth in technology, the digital economy, and society. The Department stands ready to work with this Committee in that effort.

That concludes my remarks, Mr. Chairman. I would be happy to answer any questions from you and other members of the Committee.