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: Promoting Security and Protecting Privacy in the Digital Age

I. Introduction

Chairman Leahy, Ranking Member Sessions, and Members of the Committee, thank you for this invitation to testify on behalf of the U.S. Department of Commerce concerning reform of the Electronic Communications Privacy Act of 1986 (ECPA). In the 25 years since ECPA was enacted, the communications and information landscape has been transformed. Although the authors of the law, including yourself, Mr. Chairman, recognized that the communications environment would be in a state of continual evolution, I doubt that anyone foresaw the scale and scope of the revolution to be fueled by mobile communications, the global Internet, and ever smaller, more powerful communications and computing devices.

I welcome the Committee's decision to hold this hearing and to begin another of its periodic reviews of ECPA. The goal of this effort, as always, should be to ensure that, as technology and market conditions change, ECPA continues to serve the original purpose articulated by this Committee – to establish "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement" to gather the information it needs to keep us safe.[1]

---

[1] S. Rep. No. 99-508, 99th Cong., 2d Sess. 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

I am especially pleased to be appearing jointly with our colleagues from the Department of Justice. The Administration has just recently launched an inter-agency effort to develop views on both commercial data privacy and a range of issues related to new information and communications technologies. While our effort is still in its early phases, we are guided by our shared belief that any legislative review of ECPA must be undertaken carefully and in a way that: (1) adequately protects privacy and builds consumer confidence; (2) addresses concerns raised by U.S. commercial firms about innovation, competition, and other challenges they face in a global marketplace; and (3) allows the government to protect the public in timely and effective ways.

I would like to talk today about the importance of digital communications innovation to the U.S. economy and society and the contribution ECPA's privacy framework has made to that innovation, and to reflect on some of the technology and market developments that may affect this privacy framework.

II. Commerce Department Initiatives to Address Internet Privacy and Innovation Challenges

President Obama has long recognized the importance of a modern communications infrastructure – including a robust, open Internet – to economic development, job creation, social interaction, and participatory democracy.[2] The President has also emphasized the need for "sensible safeguards that protect privacy in this dynamic new world."[3] That is why he has supported legislation directing the Federal Communications Commission (FCC) to develop a

---

[2] *See, e.g.*, "Barack Obama: Connecting and Empowering All Americans through Technology and Innovation," at 1-2, http://www.barackobama.com/pdf/issues/technology/Fact_Sheet_Innovation_and_Technology.pdf (Obama Technology Policy).
[3] *Id.* at 3.

National Broadband Plan.[4] It is why the President directed his Administration to develop an action plan for cybersecurity. It is why the entire Administration is moving forward to translate the values of openness into lasting improvements in the way government makes decisions, solves problems, and addresses national challenges.[5]

Because an open, innovative Internet is critical to the Nation's economic health, promoting its growth is a vital part of the Department of Commerce mission. To this end, Secretary Locke has established a Department-wide Internet Policy Task Force charged with identifying and developing a privacy and cybersecurity framework for Internet-based communications that meets the needs of the 21st Century information economy. This task force will also identify trade barriers around the world that may impede the free flow of information and commerce over the Internet. The Department's National Telecommunications and Information Administration (NTIA), with its statutory mission to advise the President on telecommunications and information policy, plays a leading role in the Task Force. The Task Force also draws on the expertise of the Department's International Trade Administration in international markets, the National Institute of Standards and Technology in innovation and technology, and the Patent and Trademark Office as, by statute, the Administration's advisor on intellectual property.

The Task Force's work on privacy began with a series of listening sessions with officials from major U.S. technology companies, advocacy groups, academic experts and businesses across the country. On April 23, 2010, it released a Notice of Inquiry on "Information Privacy

---

[4] *See Connecting America: The National Broadband Plan* (Mar. 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296935A1.pdf (*National Broadband Plan*).
[5] *See* Department of Commerce Secretary Gary Locke, "Our Open Government Plan" (Apr. 7, 2010), *available at* http://open.commerce.gov/.

and Innovation in the Internet Economy," which prompted more than seventy comments.[6] On May 7, 2010, the Task Force held a symposium on "Privacy and Innovation," in which a broad cross-section of industry, consumer groups, and privacy advocates participated. This fall, the Commerce Department will release a report with findings and recommendations on commercial data privacy issues and data breach. The Task Force is working closely with the Department of Justice, as well as other departments and agencies, in these activities.

It is worth noting that, although our Notice of Inquiry did not mention ECPA, multiple commenters volunteered the importance of reexamining the statute.[7] I would be happy to provide the Committee with an abstract of the commenters' views on this issue. Those comments, the information gathered in our listening sessions, and the Department's efforts over the past year to identify key Internet policy challenges, including privacy, inform my testimony today.

---

[6] *Information Privacy and Innovation in the Internet Economy*, Docket No. 100402174-0175-01, at 34 (filed June 14, 2010), *available at* http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf. For convenience, all subsequent citations in this document to "Comments" shall refer to pleadings filed in Docket No. 100402174-0175-01.

[7] *See* Google Comments, at 4, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Google%20Comments%2Epdf; Microsoft Comments, at 3, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Microsoft%20Comments.pdf; Digital Due Process Coalition Comments , at 1-9, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Digital%20Due%20Process%20Coalition%20Comments.pdf; AT&T, Incorporated Comments, at 15-16, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ATT%20Inc%20Comments.pdf (AT&T Comments); American Civil Liberties Union Comments, at 1-9, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ACLU%20Comments.pdf (ACLU Comments); Center for Democracy and Technology, at 5-6, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/CDT%20DOC%20NOI%20comments.pdf (CDT Comments); Computer and Communications Industry Association Comments, at 3-7, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Computer%20and%20Communications%20Industry%20Association%20Comments%2Epdf; Diedre K. Mulligan Comments, at 3, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Deirdre%20K%2E%20Mulligan%20Comments%2Epdf; Information Technology and Innovation Foundation, at 6, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ITIF%20Comments%2Epdf.

III. ECPA's Balance and the Growth in Electronic Communications

Over the past several decades, the explosion of electronic communications – notably the proliferation of broadband Internet service and Internet-based services and applications, as well as the expansion of wireless communications – has created enormous benefits for our nation. By some estimates, for example, the Internet contributes $2 trillion to the Nation's annual Gross Domestic Product (GDP) and supports some three million jobs.[8] The contribution of wireless services to overall GDP increased by more than 16 percent annually between 1992 and 2007, as compared with less than 3 percent annual growth for the rest of the economy.[9] These measures capture only part of the sweeping changes to ways of doing business and of communicating in our society.

ECPA has contributed to this growth. As Congress recognized in 1986, the absence of sound privacy protections for electronic communications "may unnecessarily discourage potential customers from using innovative communications systems" and "American businesses from developing innovative forms of telecommunications and computer technology."[10] In establishing a privacy framework for electronic communications, ECPA has created clear and predictable rules under which service providers could operate as well as a protected, trusted environment for consumers and businesses. It also ensured that law enforcement and national security personnel can get access to electronic communications, subject to judicial oversight and consistent with the Fourth Amendment and American principles. As Mr. Baker points out in his testimony, one of the values served by law enforcement use of this information is to protect

---

[8] *See* Executive Office of the President, National Economic Council and Office of Science and Technology Policy, *A Strategy for American Innovation: Driving Towards Sustainable Growth and Quality Jobs*, at 5 (Sept. 2009), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/innovation-whitepaper.pdf; J. Deighton, J. Quelch, Hamilton Consultants, Inc., "Economic Value of the Advertising-Supported Internet Ecosystem, at 4 (June 2009), http://www.iab.net/media/file/Economic-Value-Report.pdf.

[9] *See National Broadband Plan*, at 75.

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

individual privacy from cybercriminals and other malicious actors. In this way, as Congress foresaw, ECPA helped stimulate the development of the electronic communications industry and the many economic and social benefits that it has produced in the intervening quarter century.

Congress recognized in 1986 that the law should not remain static as technology, businesses practices, and consumer behavior changes: privacy protections "must advance with technology" or privacy will "gradually erode as technology advances."[11] ECPA modernized the federal wiretap statute, also known as Title III, to take into account the rise of new communications services – such as electronic mail – that barely existed when Title III was enacted in 1968. As Mr. Baker points out, Congress has amended ECPA on several occasions to ensure that changed circumstances did not disrupt the intended balance between individual privacy and law enforcement needs.

As the Committee begins its work of examining the ECPA's ongoing role in the digital communications environment, you face the question whether changes in that environment since 1986 warrant changes in the statute to preserve the balance Congress struck – and has maintained over time – between the privacy expectations of citizens and the legitimate needs of law enforcement.

At the fulcrum of that balance is a clear distinction between "content" and "non-content" information. ECPA recognizes the different privacy interests in these two categories, and allows the government access to non-content information through a less rigorous legal process. ECPA's drafters have worked to maintain this distinction, consistent with the overall balance between law enforcement and privacy interests. ECPA defines "contents;"[12] "non-content" is described in

---

[11] *See id.*

[12] *See* 18 U.S.C. § 2510(8) (contents include "any information concerning the substance, purport, or meaning of" a communications).

terms of a "record" or "other information" pertaining to a customer.[13] Congress has recognized that "transactional records from on-line communication systems reveal more than telephone toll records or mail covers."[14] Data not imagined by ECPA's original drafters, such as information created during websurfing, may currently be treated by ECPA as non-content information.

Based on the Department's public outreach, I believe that the results have generally been in accord with most users' reasonable expectations. As Mr. Baker amply documents in his testimony, moreover, reasonable and timely access to non-content information, such as a calling record, is critical to effective law enforcement. In seeking such access, the Department of Justice has hewn closely to the lines Congress has drawn between content and non-content information.

The Commerce Department is working with the Justice Department and other interested Executive Branch departments and agencies to consider whether substantive changes to ECPA are warranted to ensure that the balance struck in 1986 remains fair and appropriate under current technology and market conditions, as well as consumer and business practices. Once this process is completed, the Administration will be happy to work with the Committee and Congress on ECPA reform initiatives and offer views.

What I can do today is focus on what the Commerce Internet Policy Task Force and our agencies have identified as some of the most significant ways that changes in technology, shifts on societal use of communications, and the growth of the digital economy have altered the communications environment. ECPA must continue to provide a clear and well-marked road map for providers, law enforcement, and citizens and to enable further innovation and growth in technology, society, and the digital economy.

---

[13] *See id*. §§ 2702(c), 2703(c) (1).
[14] H. Rep. No. 103-827, 103rd Cong., 2d Sess., at 31 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511.

IV. The Changing Technologies of Electronic Communications

Growth of the Internet and Cloud Computing

In less than two decades, the Internet has evolved from a research network to a global communications platform that has transformed the way in which Americans gather and disseminate information, revolutionized the ways in which businesses develop, produce and market their products, and allowed virtually anyone with a good idea or an interesting point of view to find and build a following.[15] According to the NTIA-commissioned survey of Internet usage conducted by the Census Bureau, in October 2009, nearly 69 percent of U.S. households were connected to the Internet, as compared to 41.5 percent in August 2000.[16] The greatest transformation over the same period has been the growth of household use of broadband Internet service from 4.4 percent to 63.5 percent of households.[17] Worldwide, the FCC reports there are now 1.7 billion Internet users.[18]

As the number of Internet users has grown and the speed and capacity of transmissions pathways has multiplied, there has been a vast increase in the number and variety of online services, information, and applications. As a result, there has been a fundamental expansion in "the scope and magnitude of online data being collected and used in a wide variety of contexts" and "consumers are choosing to share an unprecedented amount of personal information with trusted parties and each other."[19]

---

[15] *See* Letter from Lawrence E. Strickling, NTIA, to FCC Chairman Julius Genachowski, in GN Docket No. 09-51, at 1-2 (Jan. 4, 2010), *available at* http://www.ntia.doc.gov/filings/2009/FCCLetter_Docket09-51_20100104.pdf.
[16] NTIA, *Digital Nation: 21st Century America's Progress toward Universal Broadband Internet Access*, at 4 (Feb. 2010), *available at* http://www.ntia.doc.gov/reports/2010/NTIA_internet_use_report_Feb2010.pdf.
[17] *Id*.
[18] *National Broadband Plan*, at 60.
[19] AT&T Comments, at 3-4, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ATT%20Inc%20Comments.pdf.

The global growth of cloud computing services – the ability to store data in the Internet "cloud" or to access and engage Internet-based data processing applications – is a prominent example of this phenomenon that is changing the ways we use and store information. The range of cloud-based services and applications available today and the pervasiveness of their use by consumers and businesses far exceed the levels that existed in remote computing 25 years ago. According to one projection, cloud computing revenues will grow from $46 billion in 2009 to $150 billion in 2012 and, next year, 25 percent of new software deployments will be cloud-based applications.[20] According to one 2008 survey, "at least 40% of American Internet consumers, and at least 59% of such consumers in the 18-29 age range, have engaged in some form of cloud computing activity."[21]

This growth is fueled by benefits for individuals and businesses, including the United States Government. The core value proposition of cloud computing services is the ability to replace local computing and storage capability (in either enterprise or home settings) with more flexible, affordable, reliable, on demand resource pooling from remotely-hosted services with equal or greater privacy and security properties compared to what is available through local services.[22] Users of cloud-based email services, such as Gmail and Hotmail, can access their messages from any computer anywhere in the world. A cloud user never has to worry about having left a file at the office when he or she wants to work on it from home or on the road.

---

[20] Salesforce.com Comments, at 1, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Salesforce%20Comments%2Epdf.

[21] American Civil Liberties Union of Northern California Comments, at 2, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ACLU%20Appendix%20A%20-%20Cloud%20Computing%20Issue%20Paper.pdf.

[22] The Commerce Department's National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Mell and Grance, The NIST Definition of Cloud Computing, *available at* http://csrc.nist.gov/groups/SNS/cloud-computing/.

Cloud-based services enable small and medium-sized businesses to perform essential management and administrative functions without having to keep up with investment in on-site hardware and software.[23]

Despite the benefits of cloud computing, there is evidence that concerns about the privacy and security of remotely-stored content have made both the public and private sectors wary about fully migrating to using cloud computing services. A December 2009 survey conducted for Microsoft revealed that more than 60 percent of the consumers and more than 75 percent of senior business leaders questioned cited data safety, security, and privacy as the chief concerns about cloud computing. More than 90 percent of those surveyed expressed reservations about the security and privacy of personal data stored in the cloud.[24] That finding is confirmed by a 2010 Harris Interactive Poll, which indicated that of those Americans who are not interested in using cloud computing, 81 percent are reluctant, at least in part, because they are concerned about the security of their information in the cloud.[25] These early surveys reveal that users are sensitive about whether their data is secure and private, and that they are more somewhat concerned about the actions of criminals or by service providers, than about government access.[26]

Similar concerns about the securing of data become apparent in skepticism about US-based cloud computing services by foreign customers. Even some of our closest trading partners are considering limiting the cross-border flow of data to the United States in response to

---

[23] *See* Jeffrey Rayport and Andrew Heyward, *Envisioning the Cloud: the Next Computing Paradigm*, at 14-24 (Mar. 2010), *available at* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.
[24] Penn, Schoen, and Berland, *Cloud Computing Flash Poll – Fact Sheet*, Microsoft, *available at* http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc.
[25] ACLU Comments, at 3.
[26] *See* Penn, Schoen, and Berland, *Cloud Computing Flash Poll*, at slide 19, available at www.microsoft.com/presspass/presskits/cloudpolicy/docs/CCTopline.ppt.

perceived weaknesses in the U.S. legal regime for data privacy, including protections against government surveillance.[27] The Commerce Department believes that American common law, our Constitution, and the body of laws – of which ECPA is one part – have erected a set of protections for the privacy of individual electronic information that is second to none. The stability and certainty provided by U.S. law in this area is evident in the growth of the digital economy. The Administration places a priority on ensuring that individual users and enterprise customers develop well-founded trust in the safety, security, and privacy of evolving cloud services, and we are confident in the due process and transparency of U.S. law. At the Department of Commerce, we are committed to working with our colleagues at Justice and members of this committee to address any misperceptions the global marketplace may have in this area.

The Growth of Online Storage of Electronic Messages and Attached Content

When an electronic message (and any attached document) arrives at the recipient's online mailbox, ECPA affords it substantial privacy protection; government may compel disclosure of the contents of that message only pursuant to a warrant issued by an independent judicial authority upon a showing of probable cause.[28] The legal status of the document changes (at least in most federal circuits)[29] on the 181st day or, more commonly, as soon as the recipient opens the message. Once either of these events occurs, the contents become a stored document

---

[27] AT&T Comments, at 18; CDT Comments, at 34-35; Salesforce.com Comments, at 2; Comments of the United States Council for International Business, at 3 (filed June 14, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/United%20States%20Council%20for%20International%20Business%20Comments.pdf. *See also* Mayer Brown, "Cloud Computing May Violate German Data Privacy Laws" (July 20, 2010), *available at* http://www.mayerbrown.com/publications/article.asp?id=9363&nid=6.

[28] Providers may voluntarily disclose content to a government entity in certain limited circumstances such as emergency situations and when evidence of a crime is inadvertently obtained.

[29] *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1075-77 (9th Cir. 2003), *cert. Den.*, 543 U.S. 863 (2004) (ECPA provides warrant protection for opened emails under many conditions).

that – like content held on behalf of a subscriber by a provider of remote storage or data processing – the government can access via a court order issued upon a documented showing of relevance or by a subpoena.[30]

These varying levels of privacy protection were the product of careful legislative deliberation in 1986, when the notion of remote computing (as a precursor of today's cloud computing) was anticipated by the drafters of the 1986 Act. In the new world of cloud computing, and the exponential increase in the use of email, texts, tweets, and Facebook postings, attitudes and practices may have evolved.[31] These changing business and consumer practices raise questions about what privacy expectations are reasonable and whether additional protections should be mandated by law.[32] In this regard, I agree with Mr. Baker: Technology has evolved and it is natural to ask whether changes to ECPA are appropriate.

Furthermore, as communications networks and digital information systems become more sophisticated, they not only store more content – including voice, text, video -- but also they record in greater and greater detail records of the interaction between individual users and that content. This realm of 'transactional records' was originally defined by telephone calling records and simple logs of emails sent and received. Today, the volume and complexity of those records has grown with the diversity and granularity of new service offerings available through the Internet, mobile phone networks, and the cloud. These records play a critical role in enabling innovation in the digital environment. Records of web search terms enable those providing

---

[30] When the government seeks to obtain a document without a warrant, it must give notice to the affected user. That notice, however, can be delayed, under certain conditions, for as many as 180 days.

[31] *See* Google Comments, at 4 (advent of cloud computing "is leading to a vast migration of data from personal computers, filing cabinets, and offices to remote third-party servers"); J. Beckwith Burr, "The Electronic Communications Privacy Act of 1986: Principles for Reform," at 8-9 (Mar. 2010) , *available at* http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

[32] CDT Comments, at 35.

Internet search services to increase the relevance of search results returned to individual users based on their prior browsing history. Data on the location of a given mobile device help network and applications providers to offer more customized service. And logs of our interactions with files and data in the cloud help to troubleshoot bugs in the operation of cloud services. These same transactional records can help both commercial service operators and law enforcement agencies to detect security breaches based on noticing anomalies in patterns of information usage and access recorded in these logs.[33]

Growth of Wireless and Location Services

The Federal Communications Commission issued its first group of cellular radio licensees only a few years before ECPA's enactment and few anticipated then the future of wireless communications. According to the FCC, today there are some 4.6 billion mobile phone subscribers worldwide.[34] In the U.S. alone, roughly 91 percent of the population has a wireless phone.[35] The use of smart phones in the United States grew by roughly 50 percent from 2008 and 2009, with sales expected to eclipse traditional cellular phone sales in 2011, shifting the balance toward these more powerful devices.[36] The FCC has concluded that mobile networks will be the next generation of Internet users, as smart phones enable those with mobile access to experience the benefits of Internet connectivity.[37] This will expand both penetration and usage of the multiplying range of services and communications available online.

The expansion of advanced mobile phone usage also provides unique new data streams. When turned on, cell phones and other wireless communications devices are in nearly constant

---

[33] Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler, Sussman, Information Accountability, *Communications of the ACM*, Jun. 2008, 82-87.
[34] *National Broadband Plan*, at 60.
[35] CTIA Quick Facts: Year End 2009, http://www.ctia.org/media/industry_info/index.cfm/AID/10323.
[36] *See* Roger Entner, Smartphones to Overtake Feature Phones in U.S. by 2011, Nielsenwire, *available at* http://http://blog.nielsen.com/nielsenwire/consumer/smartphones-to-overtake-feature-phones-in-u-s-by-2011/.
[37] *See* National *Broadband Plan*, at 60.

communications with nearby cell towers. In areas where there are multiple towers, a device may communicate with several towers at the same time. Notably, information about a wireless phone's general whereabouts is essential to providing cellular service. In many cases, such general location information may be supplemented by precise Global Positioning Satellite (GPS) data. Many third-party applications providers are developing innovative services based on the increased availability of real-time location data from carriers and devices themselves. Clarity of rules in this emerging area is critical for the successful development, deployment, and adoption of location-based services. Just as some of today's technologies were unanticipated 25 years ago, I am sure new developments will emerge that we cannot foresee today.

V. Conclusion

Thank you again for inviting the Department of Commerce to testify on this important issue. Over the last 25 years, there have been wholesale changes in the ways Americans use electronic communications, as well as a pervasive shift in the amount of sensitive information that we entrust to third parties. I applaud this Committee's decision to examine ECPA once again to ensure that the fair balance of reasonable law enforcement access, individual privacy protection, and clarity for service providers and customers first established in 1986 is preserved in the face of changing technology. The Department stands ready to work with this Committee as your process goes forward.

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