STATEMENT OF BRAD SMITH
GENERAL COUNSEL
MICROSOFT CORPORATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

HEARING ON ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

"THE NEED FOR ECPA REFORM AND ADVANCING CLOUD COMPUTING"

SEPTEMBER 22, 2010

Chairman Leahy, Ranking Member Sessions, and honorable Members of the Committee, my name is Brad Smith, and I am the general counsel and senior vice president for Legal and Corporate Affairs at Microsoft Corporation. In this capacity, I am responsible for the company's overall legal function, along with its government affairs and philanthropic work.

Thank you very much for this opportunity to discuss Microsoft's perspectives on the Electronic Communications Privacy Act (ECPA) and how the reform of this law can help promote security and protect privacy in the digital age. At Microsoft, we consider an updated ECPA to be key to realizing the full potential of exciting new computing technologies that allow users to collect, digitize, and store unprecedented amount of information online. These technologies, which are often grouped together under the heading of "cloud computing," are helping to reinvigorate our economy by enhancing productivity, empowering small businesses and enterprises of all sizes, and creating jobs. They are also generating whole new forms of social interaction and unleashing the power of information in rich new ways.

At the same time, these advances raise important and sometimes even profound new questions about the privacy and security of data stored in online services. As an industry, we recognize that enterprises and individual consumers will use new technologies only if they have confidence that their information will be reasonably protected. As companies, we see that the economic benefits of investment and potential for innovation will be fully realized only if clear and up-to-date privacy laws protect confidential information. And as individuals, we want to ensure that one of the most valued benefits of the PC era – that computing truly was *personal* in nature – will continue to flourish as information moves from the desktop to data centers.

ECPA was passed by Congress in 1986 -- almost 25 years ago -- to establish rules to address these issues and to strike an appropriate balance among the legitimate needs of law

enforcement, the burdens on service providers, and the public's reasonable expectations of privacy. Over this period, technology has enabled individuals and businesses to move data from the desk drawer to the desktop, to networks, to the Web, and now, in greater volumes than ever before, to the cloud, but ECPA and the balance it struck have not kept pace. We urge Congress to modernize ECPA in light of advances in technology and to ensure that, once again, the law strikes the appropriate balance among these important interests.

Microsoft supports the reform principles advanced by the Digital Due Process Coalition and further urges that Congress consider these as the pillars of ECPA reform. The Digital Due Process Coalition principles will enable citizens to trust that their data will be subject to reasonable privacy protections and preserve the ability of law enforcement to develop the fundamental building blocks of their investigations. The recommended changes also will provide greater clarity for service providers who must comply with ECPA.

ECPA reform is not the only area in which legislative action is warranted in order to advance the development and benefits of these technologies. In our view, legislation also is needed to address other emerging issues relating to privacy and security holistically, and not solely in the context of law enforcement access to user data. Users have reasonable interests in maintaining the security and privacy of their data in relation to their service providers and private third parties, and the importance of data privacy and security extends beyond the United States to include information that crosses national borders. To address these concerns, we urge Congress to consider comprehensive legislation to address issues of privacy and security relating to cloud computing. This, in turn, will help ensure that consumers and enterprises fully realize the exciting benefits of new computing technologies.

I. THE EMERGENCE OF CLOUD COMPUTING AND THE CHALLENGE OF PRIVACY IN THE CLOUD

We live in an era in which unprecedented amounts of personal information are being collected, digitized, and stored online. New computing technologies are creating new benefits for consumers and enterprises, but they also are presenting important new questions for the protection of personal privacy. The computing industry, no less than consumers, needs clear and up-to-date privacy laws in order to continue to realize the benefits of new computing innovation.

With each passing year, more and more information is being collected, digitized, and stored online. This information is being harnessed with increasing computing power in new and beneficial ways that were not imagined when ECPA was first enacted almost 25 years ago. The benefits for users of these new computing technologies include greater efficiencies for organizations to customize and rapidly scale their IT systems for their particular needs, expanded access to computational capabilities previously available only to the very largest companies, better collaboration through "anytime, anywhere" access to IT for users located around the world, and new opportunities for innovation as developers move to this new computing paradigm.

For example, a Microsoft product called Health Vault is helping doctors and patients at the Cleveland Clinic manage chronic health conditions such as diabetes and heart disease, by digitizing patient data, storing it online, and making it easily accessible to patents and health care providers. Using at-home medical devices such as heart rate monitors, glucometers, scales and blood pressure monitors, patients can track their own conditions and the effectiveness of their treatments. These medical devices can then upload the patient's data into Health Vault, which incorporates the data into the patient's personal health record at the Cleveland Clinic.

Another benefit of this new "cloud" computing is scalability, or the ability of businesses to quickly increase their computing capacity to meet peaks in demand. Everyone is familiar with

Domino's Pizza. Domino's Pizza's busiest day of the year by a wide margin is Super Bowl Sunday. Orders on Super Bowl Sunday are 50 percent above Domino's next-highest peak, a typical Friday night. Rather than buy a huge amount of IT hardware and software to handle its Super Bowl demands—which would go unused the rest of the year—Domino's Pizza turned to Windows Azure to handle the excess IT needs on that day. One of the interesting parts of this story is that the application Domino's is hosting on Windows Azure is based on Apache Tomcat, an open-source implementation of various Java technologies.

Microsoft is well-positioned to comment on this technological evolution and its impact on the need for ECPA reform. We have offered Internet-based services for almost 15 years, dating back to MSN's dialup Internet service and followed by our web-based Hotmail email service. These were the early forms of so-called cloud computing: convenient, on-demand online services. Today, we offer a full array of cloud computing services to individuals as well as to enterprises, including our hosted messaging and online collaboration solutions known as Microsoft Business Productivity Online Suite and our cloud-based storage and computing resources offered via Microsoft Azure. From our vantage point, we have seen the full arc of how the technologies governed by ECPA have evolved in the years since the law was enacted.

We believe that the technological advancements driving cloud computing are tremendously exciting, but also that they raise important questions about the privacy and security of individuals' information. Even as users begin to focus less on whether their data and communications are stored locally or, instead, are accessed remotely via the Internet, they continue to care deeply about how their information is protected and kept private. For example, in a poll commissioned earlier this year by Microsoft, more than 90 percent of the general

population and senior business leaders said that they were concerned about the security and privacy of personal data when they contemplated storing their own data in the cloud.

Given these widely-shared concerns about privacy, it is important that as we move from the era of the desktop PC to the era of Internet-based technologies such as cloud computing, we ensure that users are not forced to relinquish their privacy rights or control over their data to enjoy the benefits and efficiencies that Internet-based technologies make possible.

II. MICROSOFT'S SUPPORT FOR ECPA REFORM: RESTORING THE BALANCE CONGRESS STRUCK IN 1986

> *Congressional action is needed to update and preserve the privacy protections established in the Constitution and reinforced by federal statutes passed in the 1980s. Technological change increasingly calls into question the efficacy of the provisions enacted in the Electronic Communications Privacy Act. New legislation is needed both to modernize the law and to preserve the historical balance established between the rights of the individual and the needs of the state.*

It is not surprising that issues relating to privacy have been at the forefront of public discussion about the new computing technologies that facilitate the digitization and online storage of unprecedented amounts of information. After all, the protection of privacy is an important American value. It is enshrined in the Fourth Amendment to the Constitution which, over the years, has guaranteed that we can send a letter or make a call and be secure in the knowledge that our communications will be kept private.

However, as a result of a series of court decisions, there is uncertainty about whether the Fourth Amendment applies to information that is transferred to a third party for storage or use. On the one hand, the Supreme Court has held that the Fourth Amendment is not triggered when the government inspects documents that an individual hands over to a third party for storage or

processing.[1] On the other, the Supreme Court also has held that the Fourth Amendment can protect the contents of communications, even when those communications traverse systems that are owned and operated by third parties, because users have a reasonable expectation that their communications will remain private.[2] The constitutional ambiguity for cloud computing is created by the fact that cloud technologies appear to implicate both lines of cases.

To address such uncertainties, Congress previously has stepped in and reinforced our privacy rights, including in 1986 when Congress enacted ECPA as a response to new technologies that threatened to upset the balance between the fundamental privacy rights of citizens and the legitimate needs of law enforcement to access information to protect the public. ECPA grants certain protections to user data when it is stored online, and it establishes rules that law enforcement must follow before they can access that data. Depending on the type of customer information involved and the type of service being provided, the authorization law enforcement must obtain in order to require disclosure by service providers will range from a search warrant based upon probable cause (which requires the prior authorization of an independent magistrate) to a subpoena (which does not).

While this law has served us well for many years, continual advances in technology—most particularly the advent of low cost Internet-based computing and storage services—have called into question whether ECPA is adequate to meet our needs as a society today and into the future. For example, under ECPA, emails stored for less than 180 days receive greater privacy protections than emails stored for a longer period. And while information stored on a hard drive

[1] *See United States v. Miller*, 425 U.S. 435 (1976) (holding that the Fourth Amendment does not apply to an individual's personal records that are held by a bank).

[2] *See Katz v. United States*, 389 U.S. 347 (1967) (holding that the contents of telephone communications are protected by the Fourth Amendment).

would be fully protected by the Fourth Amendment, under ECPA a single email might be subject to multiple legal standards, depending upon whether it is stored and waiting to be read or whether it has been opened. While treating emails differently in these circumstances might have made sense in 1986, it is no longer justified in light of unprecedented digitization and indefinite storage of personal information online.

Another example involves the addition of online services to traditional desktop software – such as Microsoft Office. In Office 2010, when a user creates a Word document or an Excel spreadsheet, she may choose to save it locally or in the "cloud" via Office Web Apps. Increasingly, users think less and less about these distinctions – they simply expect that they can access their documents when they need to – at any time and on any device. It would come as a surprise to these users that the level of privacy afforded to those documents differs depending on where the document happens to be stored. Their reasonable expectation of privacy does not hinge on these distinctions.

To restore the balance struck in 1986, we urge Congress to revisit ECPA in light of these technological advancements. Microsoft supports changes that will ensure that users do not suffer a decrease in their privacy protections when they move data from their desktop PCs to the cloud. We believe that the principles advanced by the Digital Due Process ("DDP") Coalition (copy at the end of this statement) will enable citizens to trust that their data will be subject to reasonable privacy protections—no different from the protections they would receive for data on their home computers—while at the same time preserving the ability of law enforcement to collect the information necessary to protect the public. The DDP Coalition principles will also provide greater clarity for providers who must comply with ECPA.

The example of stored email can help illustrate the effect of these principles. Rather than apply a range of legal standards to emails, depending on how old they are and whether they have been opened, the DDP Coalition principles would establish a uniform rule for all emails stored online: law enforcement must secure a warrant based upon a showing of probable cause. This uniform application of the warrant standard for online emails has two advantages. First, because individuals' data at home is typically accessible to law enforcement only through a search warrant, the application of a warrant standard for emails stored online accomplishes the goal of making online and locally-stored data subject to equal privacy protections. Second, because the warrant standard would be simple and applicable across the board, it provides clarity both for cloud service providers that must comply with the warrant and for users who store their data with cloud computing services.

In advocating for these changes, Microsoft is in no way seeking to minimize the legitimate needs of law enforcement investigators in obtaining access to data in the cloud. Every year, we dedicate significant resources to working with and training law enforcement officers, agents, and prosecutors at the federal, state, and local government levels. We see and understand how important electronic information is for law enforcement, and emphasize that it is our goal to ensure reasonable privacy protections for online data that do not interfere with law enforcement's legitimate needs. While we believe that the DDP Coalition principles accomplish this goal, we view them as a beginning, not the end, of the discussion. We look forward to engaging with the Committee, other Members of Congress and all stakeholders in the effort to restore the balance among the rights of individuals, the obligations of service providers, and the needs of law enforcement that was the underpinning of ECPA in 1986.

III. ECPA REFORM IN THE BROADER CONTEXT

ECPA reform is not the only area in which legislative action is warranted. Legislation is also needed to address other emerging issues relating to privacy and security as parts of a cohesive whole, and we need to consider them not only with respect to data in the United States but with respect to information that crosses national borders.

As Congress considers reforming ECPA, it is important to recognize that the new computing technologies that are driving the need for ECPA reform also implicate other policy issues. Accordingly, it is important to situate ECPA reform in the context of a broader policy agenda that should be advanced to ensure that the full benefits of cloud computing are realized. Such an agenda would encompass not only user privacy interests in relation to parties other than the government (such as the cloud provider itself and private third parties), but also other interests that are inextricably linked with privacy, including security, transparency, and national sovereignty.

1. ***Security***. Although the cloud is being built with powerful and unprecedented security safeguards, the aggregation of data in cloud datacenters presents new and rich targets for hackers and thieves. All stakeholders must work together to protect the security of the cloud. At the same time, Congress should ensure that the penalties for launching an attack on cloud computing infrastructure are sufficiently severe to help deter would-be criminals.

2. ***Transparency***. It should not be enough for service providers simply to claim that their services are private and secure. Customers should be provided with information about why this is the case so that cloud computing users can make informed decisions about the services that best fit their needs.

3. ***National Sovereignty***. In recent years, there has emerged a global thicket of competing and sometimes conflicting laws impacting cloud computing. These laws can place cloud service providers in a Catch-22, where the decision to comply with the lawful demand for data in one jurisdiction can risk violating the data privacy laws of another jurisdiction. This situation needs to be remedied.

Microsoft believes that these issues are interrelated and thus are best addressed in concert. That is why we have advocated for consideration of legislation that would:

- require transparency around cloud service providers' security and privacy practices, including by requiring that cloud service providers maintain a comprehensive written information security program with safeguards appropriate to the use of their services, provide a summary of that program to potential customers, and disclose their privacy practices to any customer from whom covered personal information is collected;

- ensure greater rigor in the federal government's procurement of cloud services by requiring federal agencies to evaluate and select providers based in part on an assessment of their information security programs;

- enhance criminal enforcement of computer crimes targeting cloud computing data centers, and allow cloud service providers to bring suit against violators directly to augment deterrence of such crimes; and

- encourage the federal government to engage in international efforts to promote consistency in national laws governing privacy, security and government access to cloud data.

With the benefit of a modernized regulatory framework, including an updated ECPA and these complementary reforms, industry will have the solid grounding to deliver on the promise of cloud computing for both individuals and organizations.

IV. CONCLUSION

One of the principal benefits of the personal computing revolution has been that it truly has made computing more personal in nature. It has empowered individuals to use technology in the way they choose. It has allowed them to store their information where they choose. And, critically, it has given individuals the freedom to share information when they choose and with whom they choose. With this freedom, users embraced the PC and moved their personal information—documents, photographs, and communications—from their desk drawer to their desktop PC.

Now, thanks to a new revolution in computing technology, users are able to collect, digitize, and store unprecedented amounts of personal information online. Given these trends, updating America's privacy laws as they apply to the online environment is a timely and crucial objective. Microsoft believes that ECPA can be reformed in such a way that consumers will feel

confident in the privacy of their data stored in the cloud without compromising the legitimate interests of law enforcement in obtaining the information necessary to carry out its responsibilities. By responsibly reforming ECPA, we can restore the balance between the rights of individuals, the obligations of service providers, and the needs of law enforcement that motivated Congress to pass ECPA in 1986.

We also believe that ECPA reform should be one aspect – albeit an important one – of a broader policy agenda that more comprehensively addresses new issues relating to privacy and security of data in the cloud computing environment. For this reason, we support consideration of legislation that would improve transparency around security and privacy practices to ensure that users can make informed decisions on the use of cloud computing services.

Thank you for providing Microsoft the opportunity to testify today. We appreciate the Committee's leadership on these important issues, and we look forward to working with you to promote security and protect privacy in the digital age.

DIGITAL DUE PROCESS COALITION PRINCIPLES

Overarching goal and guiding principle: To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.

These principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA.

- A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations.

- A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.

- A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).

- Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.

Source: http://www.digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163