STATEMENT OF MICHAEL HINTZE
ASSOCIATE GENERAL COUNSEL
MICROSOFT CORPORATION

BEFORE THE
SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

"REALIZING THE BENEFITS OF CLOUD COMPUTING: MICROSOFT'S PERSPECTIVE ON ECPA REFORM"

SEPTEMBER 23, 2010

Chairman Nadler, Ranking Member Sensenbrenner, and honorable Members of the Committee, thank you for the opportunity to discuss Microsoft's perspectives on reform of the Electronic Communications Privacy Act of 1986 (ECPA). We appreciate the attention and seriousness of purpose with which this Subcommittee has approached the issue of ECPA reform, and we are committed to working with you, law enforcement agencies, privacy advocates, and other stakeholders to ensure that we responsibly update ECPA for the era of cloud computing.

ECPA was enacted into law in 1986 to strike a balance with respect to an issue that new digital technologies were increasingly bringing to the fore: under what circumstances is it appropriate for law enforcement to compel telecommunications and Internet service providers to disclose customer content and account information. ECPA addressed this issue by striking a balance between the legitimate needs of law enforcement and the public's reasonable expectations of privacy.

It is an understatement to say that technology has changed since 1986. We at Microsoft have witnessed first-hand the successive revolutions in computing technologies that have transformed our economy and generated whole new forms of social interaction. Indeed, in many ways Microsoft's own history reflects this transformation: we come to the issue of ECPA reform as a provider of desktop software that has since moved into providing software for servers and networks and, from there, into hosting online "cloud-based" services.

The industry-wide move to cloud computing has enabled businesses and individuals to store online orders of magnitude more data than was the case when ECPA was first passed in 1986, including some of the most confidential and sensitive business and personal information. The law, however, has failed to keep up with changes in technology. As a result, when applied to today's online services, ECPA is complex and often unclear. More importantly, when law enforcement officials seek data or files stored in the cloud, such as Web-based e-mail

applications or online word processing services, the privacy standard that is applied is often lower than the standard that applies when law enforcement officials seek the same data stored on an individual's hard drive in his or her home or office.

The failure of ECPA to keep pace with the technological times – and the ensuing uncertainty of privacy protection in the cloud computing environment – has serious potential consequences. Users will be deterred from adopting cloud services if they do not trust that their data will be kept private and secure in the cloud. In addition, those considering whether to move a service to the cloud may hesitate to invest in innovation if the rules of the road are not clear in the context of the evolving technology. In all, the full benefits of cloud computing will not be realized without a legal structure that is up-to-date and that protects users' reasonable expectations of privacy.

To restore the balance that it struck in 1986, we urge Congress to revisit ECPA and ensure that users do not suffer a decrease in their privacy protections when they move their data to the cloud. We believe that the principles advanced by the Digital Due Process ("DDP") Coalition will enable citizens to trust that their data will be subject to reasonable privacy protections – as is already true for data stored 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 are also aimed at providing greater clarity for all stakeholders.

In recommending these changes, Microsoft also recognizes the legitimate needs of government investigators in obtaining access to data that may be stored in the cloud. We spend significant resources every year working with and training law enforcement officers, agents, and prosecutors at the federal, state, and local government level. Our Digital Crimes Unit was created to assist law enforcement with its work and provides training to prosecutors and

investigators around the world. We understand the importance of supporting lawful investigations. And, we remain committed to responding to emergency requests for assistance in matters where death or serious bodily injury is threatened even without being compelled to do so. The DDP Coalition's proposal would in no way threaten this cooperation.

Finally, as Congress takes up the important issue of ECPA reform, we believe it also should look at privacy and security issues related to cloud computing in a broader policy context. Potential users of cloud computing services are concerned not only about the privacy and security of their data vis-à-vis the government, but also in relation to their service providers and other third parties. Further, the importance of protecting privacy and security extends beyond the United States and can be impacted the laws of foreign governments. To address these concerns, we urge Congress to consider comprehensive legislation to address a range of privacy and security issues relating to cloud computing.

I. The Benefits of Cloud Computing and the Challenge of Privacy in the Cloud

We have entered a new era in computing, one in which software running on users' own PCs and local networks increasingly is complemented by applications and services accessed over the Internet from remote data centers. The technologies which have enabled this new era of computing – commonly referred to as "cloud computing" technologies – are empowering users to store unprecedented amounts of digital information online.[1] 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.*** With cloud computing, users pay only for the

[1] *See* "Building Confidence in the Cloud: The Need for Prompt Industry and Government Action for Cloud Computing," Speech of Brad Smith, General Counsel, Microsoft Corporation, at the Brookings Institution Policy Forum (Jan. 20, 2010), *available at*: http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/speech0120.doc

services they need, and they can add or reduce computing capacity nearly instantaneously. This is a tremendous advantage for those enterprises, like retailers or tax advisors, that have particularly high demand for IT services during certain times of the year.

- ***Expanded access to computational capabilities previously available only to the very largest companies.*** Because cloud services are accessed remotely, customers get the benefit of the cutting-edge computing resources of their cloud provider – without needing to upgrade their own hardware.

- ***Better collaboration through "anytime, anywhere" access to IT for users located around the world.*** Because cloud applications and data are stored offsite, cloud customers can access their data from any location that has an Internet connection.

- ***New opportunities for innovation as developers move to this new computing paradigm.*** By improving access to computing resources and reducing cost, cloud technologies lower barriers to entry and help developers create new applications and help entrepreneurs start small businesses.

Today, Microsoft cloud technology is helping doctors and patients manage chronic health conditions to improve care and reduce costs; helping NASA engage the public in piecing together images of the surface of Mars; and helping businesses of all sizes better connect with and serve their customers.

Ultimately, these technological developments have involved the shifting of more and more customer data into the online environment, with much of the data being highly sensitive and confidential information. This unprecedented migration of information is valuable for customers because it allows them to increase efficiency and reduce costs, but it also raises an important question: will moving data from my premises to a third party mean that it is no longer as private or secure? This straightforward concern is widely-shared among the public. 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.[2]

To allay users' reasonable concerns, we need clear and up-to-date privacy legislation, which will ensure that when a user decides to save a document in the cloud instead of, or in addition to, on his or her local PC, the user will not suffer any decrease in his or her privacy protections.[3]

II. The Need for ECPA Reform

This is not the first time that we have been faced with a public policy issue relating to the protection of privacy in online digital technologies. In 1986, 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. Congress also was motivated by a widely-shared sense of uncertainty as to whether our traditional source of privacy rights, the Fourth Amendment, applies to digital data that is stored online. This constitutional ambiguity extends to the present day: earlier this year, for example, in *City of Ontario v. Quon*,[4] the Supreme Court declined to address whether the Fourth Amendment applies to text messages stored online, noting that courts should exercise caution when considering the constitutional implications of emerging technologies.

At its inception, ECPA was intended to create a balance between the rights of individuals and the legitimate needs of law enforcement with respect to data shared or stored in various types

---

[2] Microsoft Corporation, Cloud Computing Flash Poll – Fact Sheet, *available at*: http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc

[3] *See* "Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing," Microsoft Corporation (Jan. 2010), *available at* http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/CAAProposal.doc

[4] No. 08–1332 (U.S. S.Ct. June 17, 2010)

of electronic and telecommunications services.[5] To achieve this balance, ECPA establishes rules that law enforcement must follow before they can access data stored by service providers. 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 a third party will range from a simple subpoena to a search warrant based on probable cause.

This framework made sense when it was adopted in 1986. However, in the intervening decades, the balance has shifted between the equities of users and law enforcement. Today, the basic technological assumptions upon which the Act was based and the nature of protection given to user data stored in the cloud have not kept pace with the unprecedented digitization and storage of online data that cloud computing has enabled. As a result, more and more sensitive personal information has fallen within the reach of law enforcement tools that require a lower standard of proof.

Microsoft comes to this issue as a provider of desktop and server software that has in recent years also moved into the provision of online services to users and organizations. As such, our history gives us a clear perspective on how technological change has impacted the application and effect of ECPA.

Take the example of email. ECPA extends greater privacy protections to email messages stored for less than 180 days than emails stored for more than 180 days.[6] This distinction might

---

[5] Congress's effort to balance these competing interests is reflected in the legislative history of ECPA. *See* H. Rep. No. 99-647, at 19 (1986) (discussing goal of preserving "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."); S. Rep. No. 99-541, at 5 (expressing the concern that ambiguity over privacy protections online might "unnecessarily discourage potential customers from using innovative communications systems").

[6] Under 18 U.S.C. § 2703(a), a governmental entity may generally require the disclosure of emails in "electronic storage" for 180 days or less only pursuant to a warrant issued on probable cause. In contrast, under 18 U.S.C. § 2703(a) and (b), the government may require the disclosure of the contents of emails that have been in "electronic (continued…)

have made sense in the late 80s and early 90s, when there were few options for users to store their messages online for more than 30 days, but it no longer makes any sense. A decade after the enactment of ECPA, in 1996, Microsoft was offering the first version of Microsoft Exchange – server and desktop software in which a user typically would download email to a local machine for it to be read and stored, after which it would no longer reside on the server. Because email typically was downloaded to a local drive to be read and stored, it was reasonable to conclude that email left with a service provider for more than 180 days was abandoned with little expectation of privacy.

Shortly thereafter, in 1997, we acquired Hotmail, a web-based email service that enabled electronic communications to be stored online, in the "cloud," for longer periods of time. This ability to retain mail online even after it is read by the intended recipient began to call into question the continuing justification of the 180-day distinction. Even then, however, the amount of online storage was quite limited. But since 1997, the amount of online storage available to consumers has progressively increased, to the point where it has become essentially unlimited, with users storing gigabytes and gigabytes of their data online. Today, users regularly store email messages and attachments, including valuable pictures, documents, and data, online for years. And users reasonably expect that this data will be just as private on day 181 as on day 179.

As these and other new technologies have evolved and been embraced by users over the past decade, user expectations of privacy have also evolved alongside them. Put simply, users consider these technologies indispensable and thus are putting more and more data online –

---

storage" for more than 180 days through a menu of options, including a warrant, a subpoena, or a special court order that involves a lower burden of proof than probable cause.

including highly confidential and sensitive information – and are seamlessly moving such data between local and cloud storage. In doing so, these users have no reason to believe – nor should they – that their data is worthy of any less protection in the cloud than when it is stored locally. Many users do not even contemplate a distinction, and, absent adequate privacy protections in the cloud, those that do may be reluctant to embrace cloud services.

For example, technologies such as Microsoft's HealthVault offer individuals and health care providers the ability to store patient records and other health-related information in the cloud. As users begin storing online their medical information, among the most sensitive and private information a person possesses, the concern that a lower standard of privacy applies for data in the cloud could very well become a significant barrier to adoption.

Similarly, Microsoft's Business Productivity Online Suite (BPOS) offering includes hosted email and online document storage for enterprise customers. These businesses routinely deal with highly confidential information including trade secrets, business plans, customer lists, and privileged documents. Enterprise users tell us that they are very concerned about the privacy implications for moving such sensitive data from local storage to remote storage. A significant part of that concern relates to the circumstances under which the government can compel disclosure of their data from third-party providers.

Another example that demonstrates how technology changes can alter people's reasonable expectation of privacy is the addition of online features to traditional desktop software. For instance, features of Microsoft Office 2010 allow users to easily choose between saving a document locally or in the cloud. The seamlessness of this feature makes the distinction between local and online storage less and less salient for users. Increasingly users expect to be able to simply access their documents when they need to – at any time and on any device. We believe it would accordingly come as a surprise to these users that the level of privacy afforded

to their documents differs depending on where the documents happen to be stored. Put differently, their reasonable expectation of privacy no longer hinges on these distinctions – nor should it.

Under ECPA, there is also ambiguity as to when law enforcement can access a user's location information. Microsoft offers Window Phone operating system software for mobile phones and other software that include a function for determining the device's physical location. The ambiguity about the privacy protections afforded location data under ECPA is a source of concern for users, who reasonably see their physical location as a private – and often highly sensitive – piece of information.[7]

In all, the quantity and variety of data stored online is orders of magnitude greater than was envisioned when ECPA was passed in 1986, and this includes some of the most confidential and sensitive business and personal information. There also is an enormous variety of online services and cloud computing offerings – provided by Microsoft and a large number of other companies – that could not have been imagined in 1986. The mismatch between these new computing technologies and ECPA's outmoded distinctions is a source of reasonable concern for all stakeholders with an interest in online privacy, and it is the principal force driving the need for reform.

To restore the balance struck in 1986, we urge Congress to revisit ECPA in light of these technological advancements. We support responsible reforms that will ensure that users do not

[7] The status of location data collected through GPS devices also is uncertain under the Fourth Amendment. While some courts have suggested that there is no Fourth Amendment protection against the government using a GPS monitoring device to track an individual's movements, *see United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010), other courts have held that the Fourth Amendment protects against government monitoring for long periods of time on a 24-hour basis using a GPS device that has been attached to their vehicle. *See United States v. Maynard*, No. 08-3030 (D.C. Cir. Aug. 6, 2010).

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[8] will enable citizens to trust that their data will be subject to reasonable privacy protections – akin to 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. We believe the DDP Coalition principles also will provide greater clarity for all stakeholders. To be clear, while we support the DDP Coalition principles and believe they can accomplish this goal, we view them as a beginning, not the end, of the discussion.

In advocating for these reforms, we are not seeking special privacy protections for the cloud. Nor are we seeking to interfere in any way with the legitimate needs of law enforcement investigators to obtain the data necessary for their investigations. Indeed, we see and understand how important electronic information is for law enforcement, and we are committed to continuing to work closely and cooperatively with federal, state and local law enforcement agencies. Rather, our guiding principle is that policy decisions should be made by Congress, not by unpredictable changes in technology. Responsible reform of ECPA will restore the important balance that Congress struck in 1986 and, in doing so, will give consumers and enterprises the confidence they need to realize the benefits of this exciting new generation of computing technologies.

III. A Comprehensive Approach to Privacy and Security in the Cloud

While reconciling the competing interests of the individual and the state through a reformed ECPA is a worthy and crucial objective, it is equally important to situate ECPA reform in a larger policy context. After all, users also have reasonable expectations that their cloud

[8] See Digital Due Process Coalition, Statement of Principles, *available at*: http://digitaldueprocess.org,

service provider will keep their data private and secure with respect to entities other than the U.S. government, such as private third parties and foreign governments. To address users' reasonable expectations of privacy and security across the range of these entities, we need a holistic legislative approach. That is why Microsoft supports the enactment of comprehensive legislation that would:

1. ***Improve Privacy and Security by Guaranteeing 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. To improve transparency, legislation should require 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.

2. ***Ensure Rigor in Federal Procurement.*** Federal agencies should make their decisions regarding procurement services on the basis of accurate information about cloud service providers' security and privacy practices. To accomplish this goal, Congress should require federal agencies to evaluate and select providers based in part on an assessment of their information security programs.

3. ***Thwart Computer Criminals Who Would Target Cloud Infrastructure.*** Although the cloud is being built with powerful and unprecedented security safeguards, the aggregation of data in cloud data centers presents new and rich targets for hackers and thieves. To combat such criminals, legislation is needed that would 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.

4. ***Encourage International Cooperation***. In recent years there has emerged a global thicket of competing and sometimes conflicting laws affecting 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. Comprehensive cloud privacy and security legislation should encourage the federal government to engage in international efforts to promote consistency in national laws governing privacy, security and government access to cloud data.

At Microsoft, we believe that these issues are interrelated and thus are best addressed in concert. By enacting such legislation, Congress can create a comprehensive regulatory framework which will facilitate the adoption of cloud technologies and spur innovation and economic growth.

IV. Conclusion

Microsoft believes firmly that computing technologies work best when they give users control over their information. It should be up to users to determine what kind of documents to create, where to store them, and with whom to share them. We believe that this is one important reason why the PC revolution unfolded as it did. Consumers felt secure in the knowledge that they could move their most important documents from their desk drawer to their desktop PC and not lose any control over them.

As we experience another transformation in technology – the move from the desktop PCs and on-premises servers to the cloud – we need to ensure that the laws that govern the protection and access to information used by this technology continue to strike an appropriate balance. That is why we support the responsible reform of ECPA to ensure that users have the same privacy rights for their data in the cloud as they do for their on-premises data. Such reform would restore the careful balance that Congress first struck in 1986 when it enacted ECPA.

We also believe it is important to situate ECPA reform in a larger policy context that lays the foundation for users to embrace cloud computing in much the same fashion as they adopted the PC.

Thank you for the opportunity to testify today. Microsoft appreciates this Subcommittee's leadership, and we look forward to working with you on these important issues.