Statement of Annmarie Levins
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

"Protecting Privacy in the Cloud:

Updating ECPA for the Internet Age"

May 5, 2010

Chairman Nadler, Ranking Member Sensenbrenner, and honorable Members of the Committee, my name is Annmarie Levins, and I am an Associate General Counsel at Microsoft Corporation. In that capacity, I manage the legal support for Microsoft's U.S. and Canadian subsidiaries, directing the legal teams responsible for licensing and services transactions, anti-piracy investigations and enforcement, Internet safety work, and other areas. One of the teams that I oversee is the Microsoft Digital Crimes Unit—which is devoted to working with law enforcement to fight digital crime. Before joining Microsoft in 1998, I served in the U.S. Attorney's Office in Seattle for three years as Co-Supervisor of the Financial Fraud Investigations Unit. Prior to that, I served for seven years as an Assistant U.S. Attorney in Southern District of New York with a focus on organized crime and racketeering investigations.

Thank you for this opportunity to share Microsoft's views on reform of the Electronic Communications Privacy Act of 1986 (ECPA). We appreciate the initiative that this Committee has taken in holding this hearing, and we are committed to working collaboratively with you, consumer organizations, law enforcement agencies, and all Americans to ensure that users' privacy interests are adequately protected in the digital age. As Microsoft's General Counsel, Brad Smith, announced in a speech at the Brookings Institution in January, we support efforts to modernize ECPA and bring the statute into alignment with today's technological realities.

ECPA was passed by Congress almost 25 years ago to establish rules that govern whether and how law enforcement can compel third party telecommunications and Internet service providers to disclose customer account information and stored

communications which they hold incident to their services. The law was originally designed to strike a balance between the legitimate needs of law enforcement, the burdens on service providers, and the public's reasonable expectations of privacy.

Microsoft is in a unique position to comment on the need for ECPA reform. We have offered Internet-based services for almost 15 years, dating back to MSN's dialup Internet service. We have been offering Hotmail, our free, web-based email service, since 1997. 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, Microsoft Business Productivity Online Suite, and our cloud-based storage and computing resources, Microsoft Azure. From our vantage point, we have seen the full arc of how online services have evolved over the time since EPCA was passed in 1986.

It is our experience that the state of the law has not kept pace with developments in technology. Today, users can store documents, data, and communications to networked computers and connect to them from anywhere in the world using a wide variety of devices, including laptops, phones, and other personal electronic devices. Increasingly, Web-based accounts are used interchangeably with local storage devices. As these Internet-based resources become part of our everyday computing experiences, users may not even realize when they are using third party storage and processing capabilities. Accordingly, we believe users would be surprised to learn that the legal protections afforded their information will vary depending upon whether it is in the hands of a third party service provider at the moment the government seeks to obtain it.

Over the last 20 years, there has been a fundamental shift in the amount of sensitive information that we entrust to third parties, but the law has not shifted in kind to maintain the proper balance between the needs of the law enforcement and the public's reasonable expectations of privacy. The reason is that ECPA, the law that regulates whether and how the government can require third party Internet and telecommunications providers to disclose customer information and stored communications, relies on outdated notions of how individuals and businesses interact with information technology.

Microsoft believes that now is a critical time to address these issues. We are on the cusp of a potentially transformative age of Internet-based "cloud" computing. Cloud computing services can increase efficiencies for businesses, lower IT costs, create energy savings, and spur innovative job-creating businesses. However, unless users' privacy interests are preserved and protected to meet their reasonable expectations, adoption of these services—particularly by enterprises—may, unfortunately, be rather limited and the full potential of cloud computing may not be realized.

This is among the many reasons why Microsoft has joined a broad coalition of advocacy groups, technology companies, and academics in the launch of a new initiative—the Digital Due Process Coalition. This Coalition is focused on updating ECPA to account for the profound changes in technology over the last two decades and to ensure that users' legitimate expectations of privacy are fully respected while also taking account of the needs of law enforcement. In advocating changes to ECPA, Microsoft in no way seeks to undermine the legitimate interests of law enforcement in obtaining access to electronic data in third party hands. Rather, this coalition's efforts are intended to open a dialogue with all interested stakeholders, including the government, so that we can restore the

original balance struck by Congress when ECPA was passed in 1986 between the needs of law enforcement to conduct lawful criminal and civil investigations and the rights of our citizens to have their sensitive stored communications protected against unreasonable governmental searches and seizures.

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

We have entered a new era in computing, one in which software programs running on users' own PCs and IT systems increasingly are complemented by Internet-based cloud computing services. Microsoft has invested heavily in building a cloud infrastructure and providing cloud services because we believe they offer enormous benefits to our customers. These include greater efficiencies for organizations, including governments, 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.

As a provider of cloud computing services, we are well situated to observe both these technological advances and user's choices and preferences for cloud services. Users care that their computing services and applications function as they expect and seamlessly interoperate with other computing services and applications. Increasingly, we are moving towards a world where users will focus less on whether their data and communications are stored and processed in a hard drive within the confines of their own networks or, instead, are accessed remotely via the Internet. We believe they do—and will continue to—care deeply about how their information is protected. In a recent poll conducted by Microsoft

and Penn, Schoen, and Berland, 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.[1]

While we believe there are compelling reasons for customers to take advantage of cloud-based services that will enhance the productivity of their software, we also believe that the concerns reflected in this survey should not be ignored by policymakers. The use of cloud services invariably involves the processing and storage of data on equipment that is owned or controlled by third parties. In other contexts, such as stored bank records and telephone calling information, courts have held that the disclosure of such information to third parties (e.g., banks and telephone companies, respectively) as part of using their services may diminish a user's reasonable expectation of privacy vis-à-vis the government. While the Fourth Amendment law in this area is unsettled—particularly with regard to the contents of communications held by third party services providers—such uncertainty has the potential to undermine public confidence in the adoption of cloud computing services.

In enacting ECPA almost 25 years ago, Congress moved to affirmatively address the uncertainty of the Fourth Amendment in connection with electronic communications services and computing. While the law has served us well for many years, continued advances in technology—and in particular the advent of widely available and low cost Internet-based cloud computing and storage services—call into question whether ECPA is adequate to meet our reasonable expectations of privacy today, much less in the future. This uncertainty not only may deter users from adopting cloud services and reaping their

[1] See Microsoft Poll Fact Sheet, *available at* https://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc

benefits, but also may make businesses and other entities hesitate for fear that both their own information and that of their customers will enjoy less protection against government access than if they store the data locally. Put simply, the full benefits of cloud computing, which we believe will foster the development of innovative, job creating business models, will not be realized if users fear that data they create or store in the cloud is less private and secure than data they create or store locally.

The absence of a clear legal framework also can impact the competitiveness of online services offered by U.S. companies. It has become clear to us that foreign users—and particularly foreign enterprises—may be reluctant to use online services offered by U.S. companies for fear that data processed or stored with such services will be subject to less or uncertain protection under American law. Although a multilateral framework for law enforcement access to data in the cloud is beyond the scope of this hearing, clarifying our own laws by amending ECPA would be an important step in the right direction.

II. SUPPORT FOR ECPA REFORM

To address the uncertainty in the current scope of Fourth Amendment protection in the online world and to give potential users of cloud computing confidence that they will not suffer a loss of privacy by moving data to the cloud, we urge Congress to reform ECPA. At its inception, ECPA was intended to create a balance among the rights of individuals, the burdens on service providers, and the legitimate needs of law enforcement with respect to data shared or stored in various types of electronic and telecommunications services. ECPA grants certain protections to user data when it is transferred across or stored in such systems and 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 process law enforcement must obtain in order to require disclosure by a third party will range from a simple subpoena to a search warrant based upon 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. This shift did not result from any policy decision by the Congress; rather, it resulted from technological advancements the effect of which has been to put more sensitive personal information of individuals within the reach of law enforcement tools that require a lower burden of proof.

Quite simply, the basic technological assumptions upon which the Act was based and the nature of the protection afforded to stored electronic communications have not kept pace with the many innovations in online computing over the last 25 years. For example, ECPA extends greater privacy protections to emails stored for less than 180 days than emails stored for more than 180 days. These distinctions might have made some sense in 1986, when email services did not automatically retain messages for long periods of time. But that distinction no longer bears any relationship to reality. Hosted email and other online services regularly store emails and gigabytes of other user-generated content for years, and users today reasonably expect these communications to remain just as private on day 181 as on day 179.

Because ECPA has been overtaken by technological change, Microsoft supports the Digital Due Process Coalition's ("DDP Coalition") efforts to modernize ECPA. In particular,

Microsoft supports changes that will ensure that individuals and businesses do not suffer a decrease in their level of privacy protection when they move data from on-premises computers to the cloud.

In recommending these changes, Microsoft also recognizes the legitimate needs of government investigators in obtaining access to data 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. The Digital Crimes Unit that I oversee 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 are threatened even without being compelled to do so; the DDP Coalition's proposal would in no way threaten this cooperation.

Microsoft is not seeking special privacy protection for data in the cloud. Rather, we support focused, targeted changes to ensure that users enjoy the same level of privacy protection over data they store in the cloud as they currently enjoy when they store data locally. It is true that some actions that government agencies can take today under ECPA to gain access to information in third party hands might no longer be possible under the changes proposed by the DDP Coalition. Nothing in the DDP's proposals would, however, limit the government's power to compel the production of information directly from its owner. Moreover, the changes would rectify important inconsistencies in how the law is applied to user data and communications and would seek to create a modern set of clear and balanced rules to regulate government access to private data and communications in

third party hands. Moreover, we think that decisions about where the right balance lies should be made consciously by lawmakers after an open dialogue about the issues rather than as a result of unanticipated shifts in technology. Microsoft hopes the DDP Coalition proposal will serve as a helpful starting point for that dialogue with all stakeholders, including law enforcement.

III. CONCLUSION

Updating America's privacy laws as they apply to the online environment is a worthy 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 government agencies in obtaining access to information necessary to carry out their law enforcement 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. This will help cloud computing fully deliver on its promise of increased efficiency, cost savings, and innovation to governments, businesses, and individual users alike.

Thank you for giving us the opportunity to testify today. We look forward to working with you on this important issue.