June 10, 2010

National Telecommunications Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Dear Sirs and Madams,

I. **Introduction**:

Microsoft Corporation appreciates the opportunity to respond to the Department of Commerce National Telecommunications and Information Administration's (NTIA) Notice of Inquiry (NOI), on "Information Privacy and Innovation in the Internet Economy," as part of the Department's Internet Policy Task Force mission to identify leading public policy and operational challenges in the Internet environment.

In addition to this submission, Microsoft is also a signatory to the Centre for Information Policy Leadership (CIPL) submission. Microsoft supports the Centre's thought leadership on these issues. But, we also wanted the opportunity to provide some additional company insights to a number of the probing questions raised in the NOI. Microsoft commends the Department's efforts in conducting this inquiry and believes now is the right time for the United States to address these critical issues.

We note that the questions posed by the NOI were extremely expansive. In this submission, Microsoft will not attempt to answer all of these questions but instead hopes to provide some insight into what we consider to be some of the key questions posed by the Inquiry in Q&A format.

II. Future US Federal Policy Framework:

Q. Does the existing privacy framework provide sufficient guidance to the private sector to enable organizations to satisfy these laws and regulations?

A. We believe that now is the right time to revisit the current policy framework, both in terms of "privacy policy" but also in terms of more expansive, "information policy" as outlined in the CIPL submission. In late 2005, Microsoft, and other companies, called for a set of baseline requirements through comprehensive privacy legislation that are not specific to any one technology, industry or business model. We asserted then – as we do now – that to achieve this, baseline legislation would need to be flexible, technology neutral and can build upon the current framework of technology tools, sound

business practices, self-regulation and enforcement. Getting the balance right will also require a close partnership between industry, government, advocates, and consumers. *This NOI process is a positive step for this collective input and dialogue.* It is also important to examine these issues in the context of an increasing global focus on privacy.

Q. Are there modifications to U.S. privacy laws, regulations and self-regulatory systems that would better support innovation, fundamental privacy principles and evolving consumer expectations? If so, what areas require increased attention, either in the form of new laws, regulations or self-regulatory practices?

A. *When Microsoft and other companies called for baseline privacy protections five years ago, we suggested some very basic but fundamental guidelines be put into place. This included federal pre-emption, baseline privacy protections that applied both online and offline, increased transparency and user control over collection, use and disclosure of data and minimum security requirements. But, as the information economy has rapidly evolved, so too has our thinking around the fundamentals of information policy.*

Such a framework would necessarily build on the important protections already in place and should be framed by a clear set of information policy principles. These principles should serve as clear guidelines – rather than regulations – that define organizational accountability and align with other international privacy standards and norms. We believe the development of such principles needs to include broad stakeholder engagement and be outcomes-based, to help clarify application of privacy regulations. Taking an outcomes-based approach would help the private sector understand accountability, would isolate many of the risks associated with data, and it would give guidance to law enforcement agencies as they prioritize their efforts. To that end, enforcement should focus on harms, with the nexus on the use of the data. This is because it is increasingly difficult to track data back to the original collector. It therefore enhances consumer protection to make the use of data the nexus for enforcement rather than the collection. Finally, we believe that the current regime of functional enforcement organized – which looks at how data is used, or abused within specific industries – should remain the same.

These reasons for supporting sensible federal privacy legislation in 2005 are equally compelling in 2010. Earlier this year, we called on Congress to take a critical look at the specific security and law enforcement issues raised by cloud computing, for both consumers and enterprises. Recognizing that these issues have to be examined thoughtfully, we welcome the opportunity to work with Congress, the Administration and other stakeholders to determine the most appropriate vehicle for promoting trust and protecting user data to advance commerce and the growth of cloud computing.

While Microsoft sees an increasingly important role for basic privacy guidelines to be laid down, we have also asserted that we do not believe that legislation is a complete solution. Legislation must work in conjunction with industry self-regulation and best practices, technology solutions, and consumer education. As noted above, there are some areas, particularly with respect to emerging technologies or business models where self-regulation will ultimately be the preferred model at the outset. Search and online advertising are examples of this and we commend the FTC for establishing self-regulatory

guidelines for online advertising, as one pertinent example. Because both models create legitimate concerns about what user information is collected and for what purposes it is used, in July 2007, Microsoft introduced an enhanced set of privacy principles related to search and online advertising to ensure a greater level of transparency for consumers. Additionally, Microsoft actively engages with data protection authorities around the world to ensure that our practices meet high standards for protecting privacy.

Q. An addendum to question 2 – Cloud Computing Advancement Act (CCAA) and ECPA

For the cloud to deliver on its promise, we believe the USG needs to take responsible action to foster users' confidence that their privacy interests will be preserved and their data will remain secure in the cloud. One possible avenue we would advocate the Department and Congress consider is the introduction and eventual passage of the, "Cloud Computing Advancement Act," which would include several key elements:

- ***Strengthen privacy*** *by ensuring that users are not forced to give up their reasonable expectations of privacy when they move data to the cloud. Among other things, Congress should update the Electronic Communications Privacy Act of 1986 and related laws to account for how people use cloud technologies today and how they will use them in the future.*

- ***Enhance security*** *by increasing law enforcement resources and strengthening criminal and civil enforcement mechanisms against malicious hacking of cloud services. As a first step, Congress should amend the Computer Fraud and Abuse Act (CFAA) to make it easier for law enforcement and cloud providers to combat unauthorized access to data stored in the cloud. Congress also should provide law enforcement with the funding it needs to pursue cybercriminals.*

- ***Help users make informed choices*** *by promoting transparency around cloud providers' security practices.*

We believe that such consideration in necessary because ECPA, in particular, has been overtaken by technological change, and it no longer strikes the right balance between consumers' privacy interests and the government's legitimate need to access user information when it comes to new developments like cloud computing. For these reasons, Microsoft supports the efforts to modernize ECPA that are being led by the Center for Democracy and Technology (CDT) and has recently joined the Digital Due Process coalition to address these issues. We believe such reform is vital to bring the statute up-to-date and into alignment with current technological realities and that this should involve extensive stakeholder input.

We also believe these reforms of ECPA would complement prior calls for omnibus federal privacy guidelines. Comprehensive legislation would ensure that consumers understand and have control over the data collected about them both online and offline. In combination, omnibus federal privacy legislation, responsible reforms to modernize ECPA, and industry leadership and best practices can help create an environment that addresses users' legitimate concerns over the privacy implications of cloud computing and engenders user confidence in the cloud.

*Finally, the Administration can help **promote user confidence in the cloud** by working with other governments to agree on common approaches to jurisdiction over cloud services and data stored in the cloud—an issue that is of particular concern where cloud services transcend national borders.*

Q. Those who urge a use-based model for commercial data privacy should detail how they would go about defining data protection obligations based on the type of data uses and the potential harm associated with each use. Describe how a use-based privacy system would work?

A. *The premise of the "use and obligations" model is that the decision to **use** information creates legal **obligations** on the organization that uses the information. At a practical level, such a system may classify uses based on standard use categories. These categories might include: (A) fulfillment; (B) internal business processes; (C) marketing and selling of products and service; (D) fraud prevention and authentication; (E) research; and (F) public purposes. Irrespective of where data was collected or by whom, the obligations related to the use categories must be honored.*

Q. What is the relationship between use-based privacy rules and proposed accountability systems?

A. *The concepts are interrelated and complimentary as the obligations placed on various information uses requires organizational accountability. Under the accountability model, organizations of every size that collect or use information should assess and understand the risks that they create for others and mitigate those risks appropriately. Furthermore, promises made to individuals – including those related to complying with national laws must be honored regardless of the use, no matter where data is processed or by whom. Fundamentally, this means organizations must be transparent and answerable for their strategies to identify and mitigate risks.*

III. State Legislation

Q. What, if any, hurdles do businesses face in complying with different state laws concerning privacy and data protection?

One of the reasons Microsoft has supported the adoption of an omnibus federal privacy law is because the increasingly complex patchwork of state and federal laws resulted in an overlapping, inconsistent and incomplete approach to protecting privacy. We believe that this is both inadequate and confusing from the perspective of consumers, and unnecessarily burdensome for organizations. Additionally, widely publicized privacy lapses indicated that not all companies were adopting responsible practices for protecting the data they maintain. And these failures were leading to concerns among consumers about privacy and identify theft that threatened to erode public trust in the Internet and dampen online commerce. To illustrate the extent of this challenge, 45 U.S. states, the District of Columbia, Puerto Rico, and the Virgin Islands have each enacted their own legislation requiring notification of security breaches involving sensitive personal information. Especially for organizations committed to the proper management and use of personal information, compliance with this many different data breach regimes can prove both difficult and expensive.

IV. International Privacy Laws and Regulations

Q. What, if any, hurdles do businesses face in complying with different foreign laws concerning privacy and data protection? Q. Do foreign laws that contain content-based restrictions impede global trade or foreign investment?

See response about conflicting state laws above. Multiply this by the number of local data breach notification laws coming into effect in other parts of the globe, and compliance in this single realm becomes a regulatory quagmire.

That said, this legal patchwork has been a facet of the global privacy environment and companies like Microsoft, who have done business internationally for some time have had to come up with mechanisms to comply without interfering with business operations or trans-border data flows.

The foundation of Microsoft's approach to privacy and improved data protection is a commitment to empowering people to help control the collection, use and distribution of their personal information. One way we have implemented this is by instituting clear privacy principles and a corporate privacy policy, which together govern the collection and use of all customer and partner information, provide our employees with a clear and simple framework to help ensure privacy compliance companywide. We made sure that these principles represented the "highest common denominator" in terms of privacy protections so that every Microsoft customer, regardless of geography, would enjoy the same high level of privacy protection whether a law was implemented in their country or not. These principles also closely align with globally accepted fair information privacy principles enshrined in the OECD and APEC Privacy Frameworks. And, we believe that both companies and policymakers need to focus on where the commonalities of information policy and privacy principles exist to forge a greater level of global harmonization then focusing on differences or "adequacy standards" and the like.

Of course, there are other mechanisms that can be used to help facilitate such trans-border data flows such as through "safe harbor agreements" and "binding corporate rules" but these too have certain limitations.

In light of the ascendance of cloud computing and exponential growth in global data flows, we believe that we need to view these issues and policy solutions from a very different perspective.

To explain, we now have a fundamental tension at play. Information flows are global but privacy is local – privacy and security laws are also local. We need to question what "local" mean in this distributed global environment. Is it where the consumer resides? Where the data is stored? Where the business is registered? Or, perhaps even the jurisdictions this data may be routed through?

The "local" aspect is at fundamental tension with the complexities of information flows today, and by extension, at tension with the various players - for example, a policymaker in one economy is likely conditioned to think and prioritize "locally" despite the "global" reality of information flows. Trying to apply laws to data extraterritorially or manage trans-border data flows through corporate binding rules or contracts may prove to be even more challenging – if not impossible - as modern data flows become more continuous and multipoint.

*Given these challenges, we believe a privacy governance model based on **accountability** which requires that businesses take ownership and responsibility for the management of information – regardless of where it resides or is processed – is an important consideration. This is important because industry would like predictability and consistency and to clearly understand it's "accountability" responsibility. It is also important for policymakers and regulators everywhere to think and act both locally and globally – and this is also a tension. This can be done by ensuring that domestic legislation is consistent with well accepted international norms; that we should be considering a range of international and regional efforts such as the APEC and OECD efforts or perhaps even the COE's Data Protection Convention or emerging global standards efforts. It may be complicated and difficult, but we believe it is the only way forward.*

JURISDICTIONAL CONFLICTS AND COMPETING LEGAL OBLIGATIONS

Q. **Do organizations face jurisdictional disputes as a result of domestic or foreign privacy laws? What, if any, conflicting legal obligations do companies face as a result of data privacy laws? How do companies address jurisdictional conflicts and any resulting conflicting legal and regulatory obligations? Does cloud computing, or other methods of globally distributing and managing data, raise specific issues with respect to jurisdiction of which Commerce and regulators should be aware? Have jurisdictional conflicts had any impact on U.S. consumers?**

Today, foreign governments seek access to data or other evidence located in another jurisdiction through international legal instruments, such as Mutual Legal Assistance Treaties, and through established judicial procedures such as Letters Rogatory. For providers like Microsoft, we currently store all personal data of our U.S. customers in datacenters that are located in the United States. At the same time, Microsoft is building datacenters outside the United States, and the ability to transfer data across datacenters is critical to the efficiency and reliability of cloud computing in the long term. Cloud computing does not diminish or expand a foreign government's ability to seek access to customer data through these instruments.

The complications in the cloud computing context arise because a provider may have datacenters located in multiple countries, and providers need to be able to transfer data between datacenters freely in order to maximize the efficiencies and other benefits of cloud computing. Another complicating factor is that different countries can have divergent and, at times, conflicting approaches with respect to whether and how the government should access data stored by online service providers abroad. This uncertain state of the law — along with the highly fact-specific nature of whether a government entity has jurisdiction over data — precludes any blanket statements as to exactly when foreign governments can compel production of data held by online service providers.

Any long-term solution to the problem of conflicting jurisdictional claims and inconsistent legal obligations over data stored in the cloud must involve all stakeholders and specifically include leadership from governments. The most effective solution would be the development of a multilateral framework, such as a treaty, to address jurisdictional claims and requirements in a coherent fashion. Short of a multilateral solution, governments should continue to pursue bilateral consultations and consensus

building on procedures for resolving data access and privacy issues in ways that avoid placing cloud providers under conflicting legal obligations or erode user trust in the cloud. Such bilateral cooperation might also pave the way for a longer-term, more formal solution. In the shorter term, governments should seek ways to enhance existing Mutual Legal Assistance Treaties (MLATs) to improve the speed and effectiveness of assistance between them.

Until that happens, multinational companies may be operating in very murky waters where jurisdictional issues are likely to increasingly arise. We believe that those countries those countries that work with other governments, including the United States, to develop coherent, consistent obligations are places where cloud service providers are going to feel comfortable storing data and making other investments in providing cloud services to consumers and businesses. Those are the countries that will realize the benefits of cloud computing the most quickly and the most meaningfully.

SECTORAL PRIVACY LAWS AN FEDERAL GUIDELINES

Q. How does the current sectoral approach to privacy regulation affect consumer experiences, business practices or the development of new business models?

It adds to the complexity of compliance for many organizations, confusion among consumers and it potentially results in certain gaps in the law for emerging sectors or business models. As recommended above, baseline privacy protections that apply across sectors that are not specific to any one technology, business model or sector is preferred.

Q. How does the sectoral approach affect individual privacy expectations? What practices and principles do these sectoral approaches have in common, how do they differ?

This very much depends on the consumer as well as the sensitivity of the data in question. Fundamentally, individuals have rights related to the collection and management of information that pertains to them. Those rights are contextual based on the types of data collected and used, how the data are us used, and who is using the data. Those rights may include consent, access to information, and the ability to correct or request deletion or masking. These rights should be consistent across sectors.

NEW PRIVACY ENHANCING TECHNOLOGIES AND INFORMATION MANAGEMENT PRACTICES

Please describe any other ongoing efforts to develop privacy-enhancing technologies or processes of which the Commerce Department should be aware. Is any government action needed to encourage the marketplace in this direction?

Our software products are designed to empower individuals to block unwanted communications, protect themselves from potentially dangerous online content, and control the details of their online activities. Specifically, the InPrivate Browsing and InPrivate Filtering options in Internet Explorer 8 give individuals greater control over details about their online activities. InPrivate Browsing helps prevent users' browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser, thereby leaving virtually no evidence of their browsing or search history.

InPrivate Filtering helps individuals control the elements—such as maps, ads, scripts, or images—that third-party Web sites can potentially use to track their browsing activity.

A few other examples include the SmartScreen Filter, part of Internet Explorer 8 and Microsoft's e-mail platforms, which helps identify and block intrusive communications as well as dangerous online content by notifying people when they try to visit a Web site or download software that has been reported as unsafe. Another example includes IE 8 We also offer Microsoft Security Essentials, a free download that protects against viruses, spyware, and other malicious software.

Another area that is increasingly important in this context is identity management. To get the complexities of online identity management right, we need to balance privacy and security. Microsoft believes that we have an innovative cryptographic technology called U-Prove that balances both imperatives. U- Prove enables solutions that can ensure users reveal no more than the minimum amount of necessary information needed by a given service or applications. It can also eliminate unnecessary or unwanted linking and tracing capabilities. In March, Microsoft announced the first step toward making U-Prove available for free to anyone interested. Essentially, we donated the IP and have opened the technical foundation to the community to explore so people can test the technology organically given we believe so strongly in its importance and benefits. We did this because we believe that for an identity metasystem to take hold, the associated political, economic, legal and technical forces need to be better aligned for the ecosystem to thrive.
In terms of privacy enhancing processes, Microsoft has instituted robust internal standards guided by the principles of: Privacy by default, privacy by design and privacy by deployment. We have developed a process called the Microsoft Standard for Privacy Development (MPSD) and we make this standard publicly available for other organizations to use to develop and guide their own product development and gating processes.

While we do not believe that specific privacy enhancing technologies or processes should be mandated by law, incentives and encouragement to do so should be encouraged through flexible guidelines and standards. It bears mentioning that the concept of "privacy by design" has taken hold in a number of jurisdictions around the globe, including Canada and Europe and should be considered in the context of any legislative or regulatory guidelines being contemplated in the U.S.

SMALL AND MEDIUM-SIZE ENTITIES

Q. How do existing privacy laws impact SMEs and startup companies? Please describe any unique compliance burdens placed on smaller companies as a result of existing privacy laws.

Compliance with existing laws and the building of requisite privacy processes require a certain level of investment and organizational maturity that some SMEs may not have the luxury of possessing. For SMEs conducting business inter-state or internationally, the complexity and costs will likely multiply.

Q. Are there commercial or collective tools available to address such issues? How might privacy protections be better achieved in the SME environment?

There may be some third party tools that are available. Microsoft, for instance, has published its Microsoft Privacy Standard for Development (MPSD) precisely for this reason – so that other companies could have the benefit of our experience and apply these processes and standards as they see fit. A number of SMEs also use third party trust agents, such as TrustE for both guidance and validation that they are striving to be privacy-centric organizations.

Q. Have smaller companies been unable to engage in certain types of business activities as a result of existing privacy laws?

While we cannot say for certain, we would guess that some existing and soon to be enacted laws present challenges to smaller companies. For example, while they have not been implemented yet, t*he new EU model clauses require extensive flow through of contract terms to sub-processors, as well as tracking of sub-processors, which represents a significant administrative burden. The new model clauses go into effect May 15. We're working on keeping better track of our vendors as required, but for smaller companies this could be quite difficult.*

ROLE FOR COMMERCE GOVERNANCE

How can the Commerce Department help address issues raised by this Notice of Inquiry?

The Commerce Department can help address the issues raised in the NOI by stimulating the discussion, assimilating feedback from interested stakeholders and presenting the ideas to Congress. Additionally, DOC can help guide discussions and leadership with policymaking bodies and multi-lateral organizations like the OECD and APEC to ensure greater levels of consistency and harmonization across borders, help drive solutions and/or adjudicate around jurisdictional and cloud issues and provide privacy leadership for the US abroad.

CONCLUSION

Microsoft appreciates the opportunity to contribute to the Department of Commerce's work to encourage the appropriate balance between privacy and innovation in the information economy. We look forward to continuing our engagement with the Department on these important policy issues and please do not hesitate to contact us should you need further information or clarification of these comments. Please direct any questions to Peter Cullen at pcullen@microsoft.com or Julie Inman Grant at juliei@microsoft.com.