

Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052-6399

Tel 425 882 8080  
Fax 425 936 7329  
<http://www.microsoft.com/>



JANUARY 28, 2011

VIA HAND AND E-MAIL DELIVERY

National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 4725  
Washington, DC 20230

*Re: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*

Dear Sirs and Madams:

Microsoft submits these comments in response to the Internet Policy Task Force's request for feedback on its privacy green paper, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" ("Green Paper"). Microsoft commends the Department for launching its Privacy and Innovation Initiative and for its successful symposium on May 7, 2010, exploring the issues of privacy and innovation. Given our long-standing commitment to privacy and data security, Microsoft welcomes the opportunity to participate in this important dialogue and to work with the Department, consumer advocates, and others in industry to develop a dynamic policy framework that will withstand rapid technological advances while fostering innovation in the Internet economy.

## **I. INTRODUCTION**

Microsoft applauds the Department for appropriately recognizing the key role that Internet technology has played in driving the U.S. economy and the importance of innovation not only with respect to developing new technologies and business models, but also to designing privacy-enhancing tools. It has become increasingly evident, however, that dramatic and rapid technological advances are testing how the fundamental principles that underpin consumer privacy and data protection law — such as notice, consent, reasonable security, and data retention — should apply.

The explosive growth of the Internet, cloud computing, the proliferation of computers and handheld mobile devices, and the expansion of e-commerce, e-government, e-health and other web-based services have brought tremendous social and economic benefits. Technological advancements and increased computing power have benefited both businesses and consumers, both online and offline. At the same time, however, these technologies have fundamentally redefined how, where, and by whom data is collected, used, and shared.

The challenge for industry and governments to address together is how to best protect consumers' privacy and data security while enabling innovation and facilitating the productivity and cost-efficiency offered by new business models and computing paradigms. To help address this challenge, the Department's policy framework must achieve two ends. First, it must afford consumers robust privacy protections, while at the same time enabling businesses to develop and offer a wide range of innovative products and services. Second, it must be designed to withstand the rapid pace of technological change so that commercial data is protected not only today, but also in the decades to come.

To achieve these two ends, the proposed framework should be tested against certain fundamental criteria, among them:

- *Flexibility*. The framework should be flexible in order to permit businesses to develop innovative privacy technologies and tools. Flexibility means that businesses can adapt their policies and practices to match the contexts in which commercial data is used and disclosed and the type of relationship that they have with the consumer.
- *Certainty*. In addition to being flexible, the framework must provide businesses with certainty about whether their privacy policies and practices comply with legal requirements. Government-recognized safe harbor programs are one way in which the framework can remain flexible but also provide businesses the certainty necessary to encourage the development of innovative privacy protections and new products and services. The framework also can promote certainty by seeking harmonization with international standards and focusing enforcement efforts on cases that result in measurable consumer harms.
- *Simplified data flows*. Today, commercial data regularly flows across state and national borders, is shared within company affiliates and with vendors that manage the data on behalf of the company, and may be transferred to third parties that use the data, for example, to provide consumers with information about products and services that may be of interest to them. The framework appropriately acknowledges this reality and promotes efforts to harmonize international laws in order to facilitate the data flows that are necessary to enable more efficient, more reliable, and more secure delivery of services to consumers at lower prices.
- *Technology neutrality*. There is no question that technology will continue to change — and change rapidly. Consequently, the framework should avoid preferences for particular services, solutions, or mechanisms to provide notice, obtain choice, or protect commercial data. Preference for one privacy tool over another, for example, could chill innovation by deterring providers from developing alternative or improved approaches for protecting commercial data.

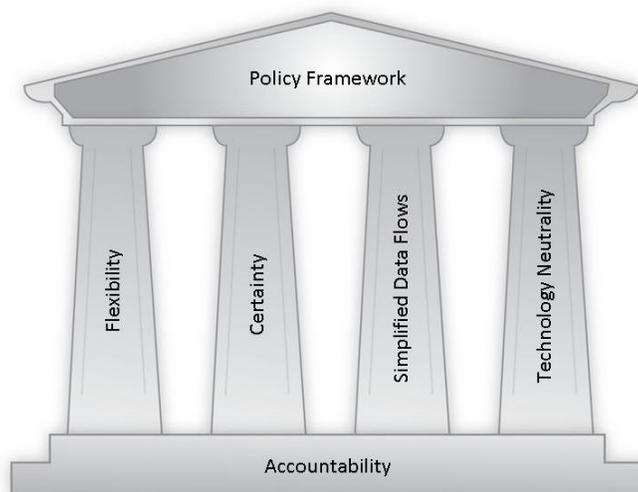
In addition, accountability must serve as the foundation for the Department's policy framework.<sup>1</sup> Accountability demands that businesses meet privacy goals based on criteria established in

---

<sup>1</sup> Additional information about the concept of accountability is available at <http://www.hunton.com/Resources/Sites/general.aspx?id=330>.

current public policy, but permits businesses to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies, and the demands of their customers. By focusing on achieving substantive outcomes, rather than imposing prescriptive rules that may be of limited effect or that may burden businesses without yielding commensurate privacy benefits, the Department’s policy framework will be more robust and resilient to technological change.

This overall approach to the Department’s policy framework is illustrated in the following diagram. The framework is supported by a foundation grounded in the concept of accountability. Building on this foundation are the four criteria by which the overall policy framework is measured: (1) flexibility, (2) certainty, (3) simplified data flows, and (4) technology neutrality. These criteria support the framework itself, and, in this manner, industry, the Department, and other relevant stakeholders can achieve the ends of affording consumers robust privacy protections that can withstand the test of time, but that still enable businesses to offer a wide range of innovative products and services.



In the remainder of these comments, we respond to the questions raised by the Task Force in Appendix A of the Green Paper, applying the four criteria identified above and the concept of accountability to help develop a dynamic consumer privacy framework. As a company that has been focused on consumer privacy for many years and that has built privacy into the way we design our products and services, we hope our comments provide the Department with helpful feedback and useful illustrations that might be more generally considered within the framework.

## **II. MICROSOFT’S COMMENTS TO SPECIFIC QUESTIONS RAISED BY THE TASK FORCE**

### **A. Enforcement of Privacy Principles (Questions 1, 3, 9(c))**

The Task Force recommends the adoption of a baseline commercial data privacy framework that is built on an expanded set of Fair Information Practice Principles (FIPPs). Microsoft is generally supportive of this approach. As we explained in our comments on the Department’s Notice of Inquiry, Microsoft was one of the first companies to call for comprehensive privacy legislation that sets

forth baseline privacy protections that are not specific to any one technology, industry, or business model.<sup>2</sup> We believe such legislation should apply both online and offline and should include baseline requirements for transparency, consumer control, and security. In addition, this legislation should create legal certainty by preempting state laws that are inconsistent with federal policy and promote accountability by ensuring that all businesses are using, storing, and sharing commercial data in responsible ways while still encouraging companies to compete on the basis of more robust privacy practices.

As explained in our earlier comments, however, legislation is not a complete solution.<sup>3</sup> While legislation is an appropriate vehicle for setting flexible, baseline standards, it is difficult for legislation to keep pace with evolving technologies and business models. Legislation must work in conjunction with industry self-regulation and best practices, technology solutions, and consumer education. Thus, Microsoft strongly supports the notion that privacy legislation should include safe harbors whereby a company that complies with a self-regulatory program approved by the FTC is deemed to comply with statutory requirements. These voluntary codes of conduct, which Microsoft agrees should be developed through open, multi-stakeholder processes, can build upon baseline statutory requirements, but can better address and adapt to emerging technologies and rapidly evolving business models.<sup>4</sup>

Microsoft believes that any comprehensive federal privacy legislation should provide the FTC and state attorneys general enforcement authority to help ensure that businesses remain accountable. Specifically, the FTC should be authorized to enforce violations and seek civil penalties, and, where the FTC has not acted, state attorneys general should be authorized to take action against violators on behalf of state residents. Microsoft does not believe, however, that a general private right of action for members of the public is necessary or appropriate. A private right of action would create both uncertainty for businesses and unnecessary litigation costs, without a corresponding benefit for consumer privacy.

## **B. Transparency and Accountability (Question 2)**

The Task Force asks a number of questions about the best ways for promoting transparency and accountability so that consumers can make informed choices about their data. Microsoft has been at the forefront of industry efforts to promote transparency.

We have found that transparency requires a careful balance between providing specific, accurate and complete information, drafting disclosures to be easily consumable and understandable,

---

<sup>2</sup> Microsoft Comment, at 1, <http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Microsoft%20Comments.pdf>.

<sup>3</sup> *Id.* at 2.

<sup>4</sup> Of course the development of voluntary codes of conduct and other self-regulatory initiatives should include consideration of appropriate and effective enforcement mechanisms. Depending on the context, these could include either (or some combination of) self-certification, enforcement by an industry association or other self-regulatory body established as part of the program, or enforcement by the FTC or state attorneys general based on the idea that non-compliance by a company that claims to adhere to the code is a deceptive trade practice.

and providing them at a time and in a manner where they are most likely to be noticed and understood. Thus, Microsoft has sought to provide privacy information through a variety of methods. For example:

- Microsoft was one of the first companies to adopt “layered” privacy notices. The Microsoft Online Privacy Statement provides consumers with the most important information about our privacy practices in a concise, one-page upfront summary with links to additional layers that describe in more detail our data collection and use practices, which includes the concepts of purpose specification and use limitation.<sup>5</sup>
- In the context of online behavioral advertising, Microsoft has supported, and is in the process of implementing, the recently launched Self-Regulatory Program for Online Behavioral Advertising, which includes placing an “About our ads” link on the bottom of pages that serve ads or collect data used for behavioral advertising and displaying a standardized text link or icon prominently in or next to ads. By clicking on the text link or icon, consumers can easily learn about online behavioral advertising and the privacy practices associated with the particular advertisements they receive, and they can opt out of behavioral advertising if they choose.
- Microsoft has successfully employed in-context, or just-in-time, notice in many of our products and services. For example, Windows Phone 7 includes a geo-location feature that enables consumers to take advantage of the increasing array of location-based applications and services on the market. However, before an application may gain access to a consumer’s location information, the consumer is provided clear notice and is asked to provide affirmative consent.
- In an effort to further increase transparency, Microsoft has also published detailed information about privacy practices in white papers,<sup>6</sup> audit reports,<sup>7</sup> and various other forms.

As noted above, there is no one-size-fits-all approach to effectively providing notice and increasing transparency. Privacy statements are not always the only, or the best, way to convey important information about privacy practices to consumers.<sup>8</sup> For some companies and in some

---

<sup>5</sup> See <http://privacy.microsoft.com/en-us/default.aspx>.

<sup>6</sup> See, e.g., “Privacy Protections in Microsoft’s Ad Serving System and the Process of ‘De-identification,’” available at <http://www.microsoft.com/privacy/policymakers.aspx>.

<sup>7</sup> See, e.g., [http://www.jeffersonwells.com/DefaultFilePile/ClientAuditReports/Microsoft\\_PF\\_IE7\\_IEToolbar\\_Feature\\_Privacy\\_Audit\\_20060728.pdf](http://www.jeffersonwells.com/DefaultFilePile/ClientAuditReports/Microsoft_PF_IE7_IEToolbar_Feature_Privacy_Audit_20060728.pdf).

<sup>8</sup> It is widely noted that full privacy statements are not frequently read by consumers. This realization often leads to calls for privacy statements to be shorter in an effort to make it more likely consumers will read them. But consumers are not the only audience for a privacy statement, and providing notice to consumers is not the only purpose they serve. They also create greater accountability. Regulators can read them and hold companies accountable under existing laws governing unfair and deceptive trade practices. Privacy advocates and journalists can use them to compare practices among different companies. But these accountability objectives can be achieved only if the privacy notices are complete and sufficiently detailed – and that sometimes means they can be (continued...)

circumstances, privacy impact assessments (PIAs) can be a useful internal tool for evaluating the privacy impact of a new technology, but they may not be appropriate as a meaningful way to convey information to consumers.<sup>9</sup> And while such so-called just-in-time notices provide an effective way to provide notice in many contexts, in other contexts this approach can prove to be too disruptive to the consumer's experience, and other methods may be more effective.

Business models and technologies may be complex, evolve quickly, and involve multiple entities that collect and handle data. Further, there is a wide variety of user interfaces and device functionality in, for example, personal computers, televisions, and mobile devices. As a result, any transparency requirements should be flexible and leave room for innovation. Standardization may only stifle attempts to innovate in ways that foster transparency. For these reasons, standardized or machine-readable approaches for privacy notices have not proven to be widely useful or successful. Overly prescriptive rules requiring standardization of privacy notices may lack the flexibility needed for diverse and rapidly-evolving technologies and business models. Further, creating prescriptive and inflexible rules in this area is unnecessary, since the FTC can and does address material failures by companies to provide accurate information about the purposes and uses of the commercial data they collect under Section 5 of the FTC Act.

### **C. Role of the Commerce Department (Question 4)**

The Task Force has recommended that the Department establish a Privacy Policy Office (PPO) to serve as a center of commercial data privacy expertise. We agree that the proposed PPO could serve a valuable function by helping to facilitate the development of self-regulation and privacy-enhancing technologies. Perhaps even more importantly, the Commerce Department, through the proposed PPO, has a critical role to play in engaging in international outreach. As explained in Section II.E below, the Commerce Department is uniquely positioned to encourage greater international harmonization and cooperation, and to help preserve and enhance secure flows of information across borders.

With respect to the proposed role of the PPO in convening stakeholders to develop codes of conduct and/or privacy enhancing technologies, we would urge the Department and the proposed PPO to move cautiously and with restraint so as to encourage and permit market forces to operate. We would also encourage the PPO to coordinate closely with other agencies, including the FTC, which may be playing similar or related roles (such as the FTC's series of roundtable events that were designed to bring together stakeholders to discuss a range of privacy issues). Only when there is a consensus among stakeholders that the involvement of the PPO would be helpful and productive should the PPO step in and be available as a facilitator.

---

quite long. So shortening privacy statements in an attempt to achieve one objective may come at the expense of another. But both these objectives (effective consumer notice and accountability) can be achieved by adopting multifaceted approaches to notice and transparency.

<sup>9</sup> PIAs used in a commercial context are likely to contain trade secrets or other proprietary information. Using them as an internal compliance tool may help to uncover information that should be disclosed in a privacy statement, but simply publishing PIAs as a means to increase transparency in the private sector is not likely to be practical or useful in many cases.

As an example, and in response to the Task Force’s question about what role the Department can play in connection with the development of “do not track” technologies, the marketplace (spurred on by the FTC) is already actively developing new tools and technologies to offer consumers simplified choice.

The next generation version of our web browser, Internet Explorer 9, will offer, for example, ground-breaking “do not track” functionality, known as “Tracking Protection.” Tracking Protection gives consumers unprecedented control over the collection and use of their data online by allowing consumers to decide which sites can receive their data and by filtering content from sites that the user chooses not to view. It does so on the basis of Tracking Protection Lists that identify trustworthy and untrustworthy websites. A Tracking Protection List may include “do not call (or visit)” lists that will block third-party content, including cookies and similar files, from any site that is listed, unless a consumer visits the site directly by clicking on a link or typing its web address. By limiting calls to these websites, Internet Explorer 9 will limit the information these third party sites can collect about web users. At the same time, Tracking Protection Lists can include “OK to call” entries that permit calls to specific sites, which allows consumers to create exceptions in a given list. Anyone on the web (including consumer groups and privacy advocates, enterprises, security firms, and individual consumers) will be able to create and publish a Tracking Protection List – which is simply a file that can be uploaded to a website and made available to others via a link. Consumers can create or subscribe to more than one list if they wish, and can subscribe and unsubscribe to lists as they see fit. Internet Explorer 9 will automatically check for updates to a consumer’s lists on a regular basis. And once a consumer has subscribed to a list or lists, Tracking Protection will remain enabled across all browsing sessions; it will only be disabled when the consumer chooses to turn it off.

More recently, other browser manufacturers also have announced new do-not-track initiatives. Further, the online advertising industry has been developing and rolling out new self-regulatory initiatives that give consumers easier to use tools to be able to opt out from online targeted advertising. Given the dynamic and rapid innovation in this space, there does not appear to be a need for the PPO to spur new technology development in this area at this time.

#### **D. The Role of the FTC (Question 5)**

The Task Force appropriately recognizes that the FTC should remain the lead consumer privacy enforcement agency for the U.S. Government, but it asks several questions related to how the FTC’s enforcement role should be defined. As explained above, Microsoft has long supported comprehensive federal privacy legislation that would be enforced by the FTC. Absent new federal privacy legislation providing the FTC this additional authority, however, the FTC’s enforcement authority is necessarily limited to Section 5 of the FTC Act and other existing sector-specific statutes.

As part of its support for comprehensive baseline privacy legislation at the federal level, Microsoft has supported providing the FTC with rulemaking authority in specific, well-defined areas. For instance, it is appropriate for the FTC to have rulemaking authority for purposes of developing minimum security requirements across sectors, akin to what authority it currently has under the Gramm-Leach-Bliley Act. As it has with the G-L-B Safeguards Rule,<sup>10</sup> more broadly applicable security standards should

---

<sup>10</sup> 16 C.F.R. §314; 67 Fed. Reg. 36484 (2002).

be developed with careful consideration of the current state of the art in administrative, technical, and physical safeguards for protecting information and of the cost of implementing such safeguards. Additionally, as described in Part II.A above, Microsoft believes federal privacy legislation should include self-regulatory safe harbor provisions, and FTC rulemaking authority is appropriate with respect to the administration of those safe harbor programs.

Microsoft does not, however, support tying FTC rulemaking authority to the failure of a multi-stakeholder process to produce a voluntary enforceable code within a specified time period. Rather, Congress should create baseline standards against which the FTC must review programs seeking approval. This would create some certainty for industry and help alleviate concerns that the review process could be unduly subjective or arbitrary. Upon request by the organization(s) that created and will implement and enforce the industry code, the FTC should review and approve voluntary, self-regulatory programs to serve as safe harbors. Without prior approval of such codes, there would be uncertainty that might result in businesses being reluctant to participate in the voluntary code — and incur the related investment costs — because there would be no guarantee that the code ultimately would meet with the FTC’s approval. *Prior* approval of such codes is thus an important component of this framework.

In addition, it is worth noting that there is already a good basis under current law — Section 5 of the FTC Act — to enforce a company’s commitment to follow a code of conduct. Companies that publicly represent that they adhere to a self-regulatory program but that materially fail to meet the requirements of the program would be seen as violating the FTC Act’s prohibition on deceptive trade practices.<sup>11</sup>

#### **E. Importance of International Cooperation (Question 6)**

Microsoft fully supports the Task Force’s recommendation that the “U.S. government should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other countries’ commercial data privacy frameworks.”<sup>12</sup> Today, commercial data regularly is shared across state and international borders. An updated and more coordinated legal framework is essential in an era in which information may be created in the U.S., using software hosted in Poland, stored in France, backed up in a data center in Singapore, accessed by support personnel in India, and then accessed again for business purposes by the creators in the U.S. Increased cooperation among privacy enforcement authorities around the world is critical to facilitating the data flows that are necessary to enable more efficient, more reliable, and more secure delivery of online services to consumers at lower prices.

Such cooperation is particularly important to the development of a global framework for the cloud. There is tremendous uncertainty about which jurisdiction’s laws apply to data in the cloud and which jurisdiction can assert authority over the data (regardless of the law applied). As a result, different and even conflicting rules may apply to the same data and conduct. These challenges to broader deployment and adoption of the cloud cannot be solved by any one government. Only through government-to-government collaboration — whether through a treaty or other multilateral framework

---

<sup>11</sup> See 15 U.S.C. § 45(a)(1).

<sup>12</sup> Green Paper, at 73.

or a less formal option — can governments create the consistency among regulatory frameworks that will enable the data flows that make the cloud work.

Microsoft urges the Department, through a newly created PPO, to actively pursue international cooperation in these, and other, areas where there are barriers to data flows.

#### **F. Role of States and Data Breach Notification Laws (Questions 7 and 9)**

The Task Force questions the extent to which state privacy laws should be preempted by federal policies and makes recommendations about the role state data breach notification laws should play. Microsoft supports broad federal preemption as part of any comprehensive privacy legislation as well as any federal data security breach standard.

Just as the patchwork of differing national privacy laws around the globe creates tremendous uncertainty and confusion for businesses and consumers, the increasingly complex patchwork of state laws results 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. Especially for organizations committed to the proper management and use of personal information, compliance with so many different privacy regimes is both difficult and expensive.

In the specific area of data security breach standards, forty-six U.S. States, the District of Columbia, Puerto Rico, and the Virgin Islands each have their own laws governing the circumstances in which a data breach notification should be sent to customers. Instead of this patchwork legal landscape, an issue as important as data breach merits a uniform law that applies across the U.S. Providers should have clear rules governing breach notification, including when notice is required, the means of providing notice, and the content of such notices. We believe that a federal breach notification standard should require notice only in cases in which there is a significant risk of serious harm. Notification should not be required, in contrast, where the potential harm is nominal, such as where information is encrypted or otherwise unintelligible to those not authorized to access it. Broad federal preemption is critical here, so that there is a single set of standards and processes companies can follow in the event of a security breach.

While Microsoft supports broad federal preemption, it does not, however, believe that preemption should go so far as to reach state unfair and deceptive trade practices laws, which deal with areas beyond privacy and in which states traditionally have played an important consumer protection role. Microsoft also believes that state regulators should continue to play an important enforcement role. As described above, we support comprehensive privacy legislation that authorizes state attorneys general to bring actions against violators where the FTC has not acted.

#### **G. Role of Sector-Specific Laws (Question 8)**

Microsoft agrees with the Task Force that a “baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important

protections to Americans.”<sup>13</sup> However, Microsoft believes that the current sectoral approach to privacy regulation adds to the complexity of compliance for many organizations and confusion among consumers. It also can result in 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 are necessary to fill in these gaps, provide consistent baseline protections for consumers, and simplify compliance for businesses that increasingly operate across traditional industry sectors.

That said, important privacy lessons can be learned from our experience with sector-specific commercial privacy laws. For example, the Gramm-Leach-Bliley Act’s security framework — under which certain federal agencies were directed to establish standards for financial institutions relating to administrative, technical, and physical safeguards<sup>14</sup> — provides a good model for a flexible and technology-neutral security requirement. As part of any comprehensive federal privacy legislation, Microsoft supports targeted rulemaking authority for the FTC to develop security standards that should apply across sectors and be technology neutral.

#### **H. ECPA and Cloud Computing (Question 10)**

Microsoft strongly agrees with the Task Force that the Electronic Communications Privacy Act (“ECPA”) needs to be reviewed and updated. Microsoft supports the efforts to modernize ECPA that are being led by the Digital Due Process Coalition.<sup>15</sup> We believe such reform is vital to bring the statute up-to-date and into alignment with current technological realities.

ECPA was passed nearly twenty-five years ago to establish standards for government access to e-mail and other electronic communications when conducting criminal investigations. At that time, most Americans had never heard of e-mail, the Internet, or mobile phones. Over the years, electronic communications have evolved dramatically and have become an essential mode of interaction for most Americans. 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, often unclear, and sometimes illogical. For example, ECPA extends greater privacy protections to email messages stored for less than 180 days than it does for emails stored for more than 180 days. This approach may have made some sense when the statute was enacted in 1986 and online data storage was limited. But today, consumers store email in the cloud for years — and expect that these emails will be just as private on day 181 as on day 179.

It is vital that we restore balance to American surveillance laws as the cloud computing era evolves. The current legal framework has not been successful in garnering necessary consumer confidence. According to a recent survey commissioned by Microsoft, 90 percent of the general population and senior business leaders are concerned about the privacy and security of their personal

---

<sup>13</sup> Green Paper, at 73.

<sup>14</sup> See 15 U.S.C. § 6801(b), 6805(b)(2).

<sup>15</sup> See <http://digitaldueprocess.org>.

data in the cloud.<sup>16</sup> As people and organizations around the world move information from desktops to their mobile devices and into the cloud, they want to be assured that companies are implementing industry-leading security practices and procedures to protect their data. A balanced approach can help ensure that citizens' data will be protected; that law enforcement will have the tools they need; and that America will continue to lead in technological innovation.

We believe ECPA reform would complement omnibus federal privacy guidelines. Comprehensive legislation would ensure that consumers understand and have control over the data collected about them both online and offline. Omnibus federal privacy legislation, responsible reforms to modernize ECPA, and industry leadership and best practices, when combined, can help create an environment that addresses consumers' legitimate concerns over the privacy implications of cloud computing and can engender consumer confidence in the cloud.

### III. CONCLUSION

Microsoft appreciates the opportunity to comment on the Task Force's Green Paper and applauds the Department's focus on this important set of issues. We hope that our comments prove helpful as the Department continues to clarify the scope and application of the framework.

Please do not hesitate to contact me if you have any questions about our comments. Microsoft looks forward to working with you and other stakeholders, to continue a productive dialogue aimed at providing sound guidance to businesses and helping to ensure that consumers' privacy interests are protected as technology continues to advance.

Sincerely,



Michael D. Hintze  
Associate General Counsel  
Microsoft Corporation

---

<sup>16</sup> Mike Hintze, Restoring Balance to American Surveillance Laws (Mar. 30, 2010), [http://blogs.technet.com/b/microsoft\\_on\\_the\\_issues/archive/2010/03/30/restoring-balance-to-american-surveillance-laws.aspx](http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/03/30/restoring-balance-to-american-surveillance-laws.aspx).