Before the
UNITED STATES DEPARTMENT OF COMMERCE
Washington, DC 20230

Global Free Flow of Information on the Internet	)	Docket No. 100921457-0457-01 / 0561-02
Notice of Inquiry	)	RIN 0660-XA20

To: National Telecommunications and Information Administration

COMMENTS OF MICROSOFT CORPORATION

Microsoft Corp. ("Microsoft") supports the work of the Department of Commerce's Internet Policy Task Force (the "Task Force"), and in particular welcomes the Task Force's focus on the importance of promoting the global free flow of information on the Internet.

While the Internet has long been a global phenomenon, today more than ever a free flow of information and data on the Internet is essential to innovation, economic growth, and the well-being of societies. Unprecedented investments in data centers and other computing infrastructure, as well as increasingly ubiquitous broadband networks, have enabled the era of cloud computing in which sophisticated applications and services are provided to consumers and businesses remotely over the Internet. Yet only with the free flow of information and data can these investments bring about their full potential.

As the *Notice of Inquiry* recognizes, government has an important role in shaping and enabling information flows. Leadership by government is especially necessary to address a growing, global thicket of laws regulating user content and data held by online providers — affecting areas such as data privacy, data retention, law enforcement access to user data, and censorship. Industry has already taken steps to mitigate some of the dilemmas posed by divergent legal rules and competing claims of jurisdiction over data, but it cannot solve these problems alone. In these comments, Microsoft accordingly identifies practices limiting the free flow of information online today and offers suggestions for how governments and industry can address these issues in partnership.

I. Government Policies that Restrict the Flow of Information: Rationales and Consequences.

This submission discusses the rationales and consequences associated with three types of restrictions on the free flow of information and data: censorship and other direct limitations on content and services within a jurisdiction, limitations on data transfer to other jurisdictions, and broad assertions of jurisdiction over remote data. As discussed below, even when these laws are designed to address critical objectives such as data privacy and security, inconsistencies across jurisdictions can impede innovation, trade, and investment.

A. Censorship and Other Limitations on Content and Services Within a Jurisdiction.

Some governments directly limit the information that can be accessed by their citizens. Prohibitions on undesirable or illegal content often are intended to protect citizens from the harms associated with unlawful content — not just the harms associated with accessing the information, but also the harms associated with producing it (*e.g.*, when governments take steps to prevent illegal online

activity such as the distribution of images of child exploitation). These restrictions can take numerous forms, including blacklists of blocked sites, filtered search results, take-down notices, and civil or criminal liability for facilitating access to unlawful information.

However, some restrictions on content can be unduly broad, limiting freedom of expression and jeopardizing innovation. The Global Network Initiative ("GNI") (of which Microsoft is a co-founder) has therefore articulated the principle that "[b]road public access to information and the freedom to create and communicate ideas are critical to the advancement of knowledge, economic opportunity and human potential."[1] Microsoft subscribes to this principle, and like the Task Force, we oppose restrictions on peaceful political expression.[2] We make our views on Internet freedom known to governments, and take steps to reduce the likelihood of harm — such as by requiring proper legal authority before we remove any Internet content, by providing users notice if we do remove content as a result of a lawful request, and by removing access to content only in the country issuing the order where technically feasible. Yet the fact remains that in many countries throughout the world, Internet and technology providers are subject to laws that negatively impact privacy and freedom of expression.

In addition, unduly broad restrictions on content may discourage investment and decrease trade. Before offering certain services or making data center investments in new markets, Microsoft evaluates and assesses the markets to identify circumstances when freedom of expression and privacy may be jeopardized. If the country assessment reveals high levels of risk, it may be necessary to limit the services offered in that country or reconsider our plans to invest in that particular market.

B. Limitations on Data Transfer to Other Jurisdictions.

Governments have a role in shaping the privacy and data security rules that protect individual, commercial, and government information that flows on the Internet. Often, however, privacy and data security policies created by governments impose limitations on the export of data to other jurisdictions and thereby inhibit the free flow of information on the Internet.

Consider, for example, the Data Protection Directive of the European Union (EU). Article 25(1) of the Directive broadly restricts the transfer of personal data from the European Economic Area (EEA) to any country whose domestic laws do not provide a level of protection that the EU considers to be "adequate."[3] To date, only a few countries, such as Argentina, Switzerland, and certain Channel Islands, have benefited from formal adequacy determinations from the European Commission. Other jurisdictions outside of the EU impose similar cross-border data transfer restrictions.

In the EU's case, U.S. and European authorities recognized that the U.S. was unlikely to receive a formal "adequacy" determination from the European Commission in light of the United States' sector-specific (as opposed to comprehensive) approach to protecting personal information. They therefore negotiated a separate Safe Harbor Agreement to facilitate data transfers from the EEA to recipients in the U.S. participating in the Safe Harbor. The International Trade Administration (ITA) has

---

[1] The GNI principles may be found at http://www.globalnetworkinitiative.org/principles/index.php

[2] *See, e.g.*, Posting of Steve Ballmer to the Official Microsoft Blog, Microsoft & Internet Freedom (Jan. 27, 2010), http://blogs.technet.com/b/microsoft_blog/archive/2010/01/27/microsoft-internet-freedom.aspx

[3] The EEA encompasses Iceland, Liechtenstein, Norway, and the 27 member states of the EU.

served a valuable role in administering the Safe Harbor Agreement, facilitating its use by U.S. companies. Recently, however, some national data protection authorities in the EEA, for instance in Germany, have raised concerns about this framework. As a consequence, some European companies are unwilling to convey data to the U.S. in reliance on the Safe Harbor Agreement.

Other processes for transferring protected data from the EEA to other jurisdictions have likewise proven difficult to navigate. Multinational organizations seeking approval concerning the adequacy of their Binding Corporate Rules ("BCRs") — codes of conduct governing the transfer of personal data from an EEA member state to the organization's operations outside of the EEA — confront a complex and, at times, unworkable administrative process.[4] Likewise, European model data transfer contractual clauses, which are intended to facilitate data flows between companies in a way that conforms with European adequacy standards, often lack the flexibility needed for complex data transfer scenarios involving multiple parties and countries.

Fortunately, the European Commission (EC), in a recent strategy paper prepared as part of an EU-level review of the Data Protection Directive, has signaled its intent to re-evaluate the existing data transfer mechanisms.[5] The EC has recognized that "there is a general need to improve the current mechanisms allowing for international transfers of data" in light of technological changes since the Directive was adopted fifteen years ago.[6] It likewise has expressed a desire to "ensure a more uniform and coherent EU approach vis-à-vis third countries and international organisations."[7] The EC and other countries reviewing or considering privacy regulation could consider as a model the "accountability" approach taken by the Canadian federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA). Under PIPEDA, the organization transferring data for processing takes responsibility and remains accountable for its protection and appropriate use — regardless of whether that data is transferred across borders.[8] This approach provides a flexibility of implementation that reduces bureaucratic hurdles relating to international data transfers that inhibit the free flow of information online.

Some jurisdictions go further than the EU and impose near-complete bans on the export of certain types of data. For example, under the privacy laws in Nova Scotia and British Columbia, personal data held by public bodies in those provinces, with very limited exceptions, cannot be moved to any jurisdiction outside of Canada. Also, in many countries, public-sector procurement contracts frequently mandate that data be stored locally. Sometimes these requirements for local data storage are based on a misunderstanding of local law — where the official procuring a cloud service, for example, erroneously believes that local data storage is legally required. Sometimes the locality

---

[4] Additional information on BCRs and their role in transfer of personal data outside of the EEA is available at http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[5] *See* Communications from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A Comprehensive Approach on Personal Data Protection in the European Union* (Nov. 4, 2010), http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[6] *Id*. at 16.

[7] *Id.*

[8] *See* Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders* (January 2009), http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf.

restriction is based on a concern or misunderstanding about foreign law — in particular the extent to which foreign governments can access the data if stored outside the customer's country. Regardless, contractual limitations in government procurement can create the same kinds of barriers to the free flow of information as statutory restrictions such as those imposed in Nova Scotia and British Columbia.

Even when a jurisdiction does not intend to limit data flows, the lack of harmony in national regulatory frameworks often has the effect of undermining the free flow of information. Today, there is a patchwork quilt of data protection requirements across the globe — resulting in increased economic burdens, greater compliance costs, and reduced incentives to invest for companies that operate globally.

Regardless of the nature of the cross-border data restriction — whether it is the result of an express prohibition on data export, a limitation based upon an adequacy requirement, a government procurement requirement, or inconsistent laws across jurisdictions — the effect is to depress investment, reduce trade, and deprive consumers of the benefits of cloud computing and other innovations. Computing service providers subject to cross-border data restrictions are forced to implement cumbersome and expensive processes in order to legitimize the data transfers. Alternatively, the provider may be forced to store the data locally in the jurisdiction that imposes the export restriction, thereby eliminating one of the key efficiencies inherent in cloud computing.

C. Indirect Effects of Broad Assertions of Jurisdiction Over Remote Data.

Confronted with imperatives such as deterring cybercrime, protecting consumer privacy, and maintaining data security, governments increasingly are focused on user content and other data held by service providers — regardless of the location of the data. Multiple countries may have an interest in a single matter or policy question affecting a particular data set. As a result, many governments make broad assertions of jurisdiction over data stored in foreign jurisdictions.

Some countries take the view that only the country in which the data is stored has jurisdiction over it. Others assert jurisdiction so long as the service in question is offered there or if the user associated with the data resides there. Still others assert jurisdiction on the basis that the computing service provider has a place of business in the country, regardless of where the data or user is located. This unpredictability of jurisdictional reach can depress interest in cloud computing and other innovations, as users concerned about their data being accessed by foreign governments or otherwise governed by foreign laws may hesitate to adopt online services at all.

Cloud computing provides its greatest economic benefits and efficiencies when data is able to move freely between data centers. Uncertainty about the extent of governments' reach can reduce or eliminate these efficiencies. India, for example, reportedly has pressured RIM and other computing service providers to set up servers in India in order to facilitate local authorities' ability to monitor user communications. Yet it is both technically and financially impracticable for computing service providers to build duplicative local data centers in every jurisdiction. Potential cloud users overseas also have expressed concerns about having their data stored in the United States, due to a perception that the U.S. government can freely access their information under the Patriot Act. By limiting the locations in which users will allow their data to be stored, these concerns make cloud computing less efficient and effective than it otherwise could be.

When combined with broad assertions of jurisdiction, differences in substantive laws on key issues like data privacy, data retention, and law enforcement access also create irreconcilable obligations for computing service providers. For example, there are cases in which the data retention

rules of one country may violate the privacy rules of a second country. Similarly, service providers may face situations where the disclosure of data to one government in response to a lawful demand under that country's rules would violate the privacy laws of the country where the data is hosted. These situations put computing service providers in a classic Catch-22 situation, in which it is impossible to comply with the laws of both countries asserting jurisdiction over the data in question.

II. Industry and Government Working Together Can Enhance the Free Flow of Information and Data on the Internet.

A. Industry Efforts to Address These Challenges.

Computing service providers already have taken several steps to lessen the impact of restrictions that limit the free flow of information online. The GNI in particular highlights the benefits of industry collaboration. GNI is the leading private-sector effort to promote the free flow of information and data on the Internet. A coalition of companies, investors, and human rights organizations came together to launch the GNI over two years ago. The GNI has since issued voluntary guidelines for companies to follow when presented with government demands for censorship or access to user data. All participants agree to require that governments follow established domestic legal processes before disclosing user data or blocking local citizens' access to content. Participants also agree that they should strive to interpret government restrictions and demands for user data narrowly so as to minimize the negative effects of such demands on users.

In addition to collaborative efforts within the private sector, individual computing service providers are devoting considerable resources to ensure that their physical operations and corporate structure minimize the problems posed by conflicting legal rules — often at the expense of the efficiencies and other benefits cloud computing can provide. But these efforts cannot entirely solve the problem. For both business and technical reasons, it simply is impractical to locate servers in every jurisdiction or to strictly segregate data in multiple locations based on the presumed location of users.

As noted, industry also has worked with regulators and partners in other jurisdictions to legitimize data transfers out of jurisdictions with strict export limitations (such as the EU). The unpredictability of national regulators' willingness to accept certain compliance methods and the inflexibility of tools such as model contractual clauses, however, have limited the impact of these efforts, particularly in the context of cloud computing and other next-generation services that are inherently global in nature.

In short, the private sector alone cannot resolve the problems created by inconsistent legal frameworks for data. Companies that are physically present and operating in a jurisdiction have a legal obligation and practical imperative to comply with local law and to accede to local law enforcement demands for user data. Their refusal to do so can imperil their businesses and jeopardize the safety of their local employees. These problems will only grow as cloud computing becomes more popular. Failure to resolve these looming issues will pose dire problems for industry, consumers, and governments alike, endangering the future growth of cloud computing and the vast potential for innovation that is presented by the next generation of computing.

B. The Need for Government Leadership

While industry must play its part, any long-term solution to the problem of conflicting jurisdictional claims and inconsistent legal obligations ultimately requires leadership from, and collaboration among, governments. Many governments have attempted to establish procedures to avoid such conflicts, but the mechanisms for doing so have often faltered in practice. The reality is that

no government can solve this problem by itself. Only through government-to-government collaboration can governments create the consistency among regulatory frameworks that is necessary to enable the free flow of information online.

Today, there is an opportunity for the United States and other governments to provide greater clarity and consistency on the legal norms that will protect the privacy and security of user data while also ensuring legitimate law enforcement needs are addressed. The United States may find common partners in these efforts in the EU. Despite challenges in implementing the Safe Harbor Agreement, fundamentally the U.S. and EU member states share similar values on freedom of expression, privacy, and the delicate balance between law enforcement needs and other democratic values. A common approach on both sides of the Atlantic to promoting a globally harmonized framework could also serve as a model for future negotiations in Asia and elsewhere. While it is no easy task, those governments that take the lead in this area are likely to have a significant advantage in promoting the growth of online computing in their jurisdictions — and reaping the benefits these technologies offer for job creation, productivity, and economic growth.

There are several options worth exploring as the U.S. works with the EU and other partners in removing jurisdictional and legal barriers to the free flow of information and data.

A new multilateral framework. It may prove most effective for governments to seek a multilateral framework on these issues in the form of treaties or similar international instruments. While this option would undoubtedly require significant diplomatic leadership and resources, it offers perhaps the best hope of addressing legitimate government needs in a coherent fashion while ensuring that business and consumer interests in privacy and freedom of expression are adequately met on a global scale. The U.S. could work within an entity such as the G8 or G20 to take up this issue, and rely on multilateral organizations such as the OECD to research the problems faced and make recommendations for how to resolve them.

More active bilateral consultations. A less formal option would be for countries to engage independently in consultations and consensus building on consistent procedures for resolving data access and censorship issues. Even bilateral discussions on these issues will increase awareness of the problems and pave the way for a longer-term, more formal solution. On a case-by-case basis, these discussions also can take providers out of the Catch-22 situations in which competing demands force them to choose between violating one country's laws or complying with another country's demands. Bilateral discussions may be particularly appropriate with respect to categories of data, such as health or financial information, that are subject to additional regulatory and privacy concerns; countries could pursue a broad, multilateral framework for the privacy and security of data generally while carving out these especially complicated categories of data for further discussion and consensus building that takes account of evolving technology and practices.

Domestic reforms. Although international engagement is important, the U.S. and other countries also need to consider the impact of their domestic policies. Governments should be specific, transparent, and consistent in the demands, laws, and regulations that are issued with respect to data and information on the Internet, including in areas of free expression, privacy, security, and government access to user information. In addition to updating its own domestic framework, the U.S. should consider ways to encourage other jurisdictions — such as the EU and the Canadian provinces of British Columbia and Nova Scotia — to update local laws that unduly restrict the export of data.

In short, domestic laws should reflect the reality of 21st century computing. To that end, Microsoft supports an updating of the Electronic Communications Privacy Act (ECPA) here in the United States. While ECPA has played a vital role since the 1980s in providing Americans with statutory privacy protection for electronic and stored communication, it reflects the needs of an era in which data was stored locally rather than in the cloud. Reforms of ECPA could provide more clarity and updated standards for U.S. government access to data stored in the cloud. Importantly, an updated ECPA could serve as a model for other governments and multinational discussions. The U.S. also should ensure that there are clear federal standards governing important areas like privacy and security. Otherwise, computing service providers could be required to comply with 50 different state laws — a daunting task that could raise costs and stifle investment in the cloud.

While governments must lead these efforts to reform and harmonize laws, it is vital that all stakeholders are represented in any deliberations addressing impediments to the free flow of data and information. Thus, these deliberations should include not only representatives from government, but also representatives of industry, consumer groups, and other interested stakeholders. By working together, stakeholders can bring about rules that balance the legitimate needs of all parties and serve the common interest in innovation, commerce, and free expression online.

III. Conclusion

The Internet already has enriched economic, political, educational, and cultural experiences for people the world over. The next generation of technological advances, which will usher in new opportunities for innovation and economic growth, relies even more heavily on the free flow of information and data. At the same time, it is important to recognize that governments have legitimate interests in restricting harmful content, protecting the privacy and security of their citizens' data, and preventing crime. Consumers, businesses, and governments must work together to shape policies that will enhance the exchange of information while also advancing vital government objectives. Microsoft is committed to being part of this effort and looks forward to continued work with other stakeholders, including the Department of Commerce and its Internet Policy Task Force, to achieve this goal.

Respectfully submitted,

Michael D. Hintze
Associate General Counsel
Microsoft Corporation

December 6, 2010