TechAmerica
WHERE THE FUTURE BEGINS

TechAmerica.org

TechAmerica
601 Pennsylvania Avenue, NW
Suite 600, North Building
Washington, DC 20004
P 202.682.9110

TechAmerica Submission
Notice of Inquiry on Global Free Flow of Information on the Internet
Internet Task Force – U.S. Department of Commerce
December 6, 2010

Introduction

TechAmerica[1] commends the Department of Commerce for establishing the Internet Task Force to explore and address important issues regarding the Internet, and we appreciate the opportunity to provide our input on this Notice of Inquiry on Global Free Flow of Information on the Internet (NOI).

It is important to define what the global free flow of information is for the purposes of this submission. TechAmerica's member companies, global in nature, fuel the Internet economy. They use – or enable others to use – global networks to transact business every minute of the day. As such, the free flow of information includes the transmission of data reflecting business-to-business transactions, online commerce, mobile commerce, consumer communications, social networks, and information resources.

The U.S. is the undisputed leader in the creation, deployment, and use of information networks. As the NOI points out, "…online commerce accounted for over $3 trillion dollars in revenue for U.S. companies in 2007."[2] Given its market and economic position, the U.S. is on the forefront

[1] TechAmerica is the leading voice for the U.S. technology industry – the driving force behind productivity growth and jobs creation in the United States and the foundation of the global innovation economy. Representing approximately 1,200 member companies of all sizes from the public and commercial sectors of the economy, it is the industry's largest advocacy organization and is dedicated to helping members' top and bottom lines. TechAmerica is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing).It was formed by the merger of AeA (formerly the American Electronics Association), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics & Information Technology Association (GEIA).Learn more about TechAmerica at www.techamerica.org.

[2] *Global Free Flow of Information on the Internet*, 75 Fed. Reg. 60068, 60069 (Sept. 29, 2010) ("Free Flow NOI").

of thought leadership and public policy development in the areas that touch the Internet and electronic commerce. As a result, we expect that other countries will be influenced by the policy directions that we take here at home. Under the best construction, that emulation would move toward harmonization of policy that enables even greater use and proliferation of Internet and Internet technologies. However, we can also envision a situation in which policies developed here in the U.S. do not enable such harmonization in the global environment, or one in which other countries use the U.S. model for a basis for their own regimes, which could be implemented in more prescriptive ways that hamper our global competitiveness and the promise of the Internet for even greater connectivity, economic growth, and innovation on a global basis.

1. **Types of Restrictions on the Free Flow of Information on the Internet**

   Despite the promise of the Internet and the interconnected networks we enjoy today, there are ways in which government policymakers do and can restrict the global free flow of information on the Internet. These elements range from neglecting ways in which government policies can encourage the use of the Internet and spur its growth to more purposeful legislation or regulation that directly – or indirectly – restrict information flow, particularly across traditional borders that are not recognized by the Internet. Further, in order to preserve the functioning of the Internet in a global fashion, there is a need for a single authoritative root that includes the resolvability of all top level domain names.

   By not promoting greater adoption of products and services that enable greater use of the Internet by its citizens, a country can inhibit free flow of information. These include market restrictions on telephonic devices, computers and other hardware products (through tariffs, product specifications, or indigenous innovation requirements) as well as restrictions on the importation of telecommunications, e-commerce and value added services. This is particularly hampering to information flows when there is no local market to provide these products and services and yet foreign providers face limitations on their ability to enter or serve the market in a competitive environment.

   Governments also take proactive measures to put laws or regulations in place that can impede the flow of information. These include measures that block online services (in whole or in part) ostensibly for purposes of privacy, security, content control; allow for/require surveillance tools; have onerous licensing/usage restrictions. In some cases

the motivation for such regulation is unclear and the development of the particular regulation or legislation is not transparent or inclusive. Since electronic commerce is such a key component of the Internet economy, the ability to transmit the pertinent information and deliver the product is crucially important. If certain goods are prohibited in certain jurisdictions, for example, that hampers the ability to conduct commerce, generally. In addition, the varying rules around the world regarding information that cannot be collected and products that cannot be sold from one jurisdiction to the next make companies incur costs in their business operations. In this regard, the technology policy of one jurisdiction cannot scale globally, and the resulting patchwork of restrictions and/or requirements is prohibitive for companies' business designs.

One example of prospective lawmaking or regulation in the U.S. that would restrict the free flow of information is the Federal Bureau of Investigation's (FBI) apparent call for expanding the Communications Assistance for Law Enforcement Act (CALEA). Based on recent press reports and public statements by FBI officials, it appears that elements of a pending proposal would include requirements that communications services that encrypt messages must be able to deliver plain text to law enforcement; foreign providers that do business in the U.S. must have a domestic office capable of performing intercepts; and peer-to-peer software must be designed to be technically capable of complying with a wiretap order. These measures would have both civil liberties and economic consequences that concern our members and those in the civil society community. First, there could be a debilitating impact on electronic commerce and communications services if the consumer base believed that the government could more easily tap their personal communications. Second, the cost to companies to re-engineer their systems to accommodate such requirements could be profound. And, third, there is a concern that such a policy would hamper the competitiveness of U.S. companies in the global market on the one hand; on the other hand, other countries could see such regulatory authority in the U.S. as model for their own regime – either just as, or even more onerous for cost and concerning for civil liberties. In keeping with the tradition of an open and transparent rule-making process in the U.S., as they deliberate such proposal (pending), the FBI and the Department of Justice need to engage industry and other stakeholders in the discussion about what measures are feasible, effective, and least onerous on business models or civil liberties as is possible.

The NOI asks how the U.S. Government and the Department of Commerce, specifically, can assist U.S. entities in gaining greater access to new markets and what role the Department of Commerce can play in helping to reduce restrictions on the free flow of information over the Internet. The U.S. federal Government can assist U.S. companies in the global markets by fostering policies that enable free flow of information here at home as well as pursuing a global trade regime that supports such information flows through the World Trade Organization and bilateral trade agreements. In addition, the U.S. can align its funding for capacity building with a country's adherence to policies that will enable the free flow of information over the Internet.

The Department of Commerce can continue to utilize its foreign commercial service offices to work directly with foreign governments and U.S. companies pursuing business in foreign markets to inform policymakers and business leaders alike about the market environment and the impact of regulation or legislation. TechAmerica member companies value – and would welcome even greater interaction with the Department of Commerce's Foreign Commercial Service officers (FCO). We would also suggest that the FCOs receive adequate training for addressing technology trends and the needs of ICT and new technologies in order to understand and foster their adoption globally. Such a leadership role requires budget commitment, which TechAmerica supports. Further, the Department of Commerce can play an active leadership role in the interagency process here at home that considers national policy about Internet issues as well as continue its active engagement in international forums. The perspective that the Department of Commerce has on the economic impact of policy decisions is a critical component of those deliberations.

2. Identifying Best Practices

In the Internet Age, is it extremely difficult to comply with or enforce a global patchwork of laws and regulations that address the Internet. Traditional borders do not apply and, therefore, traditional notions of boundaries and jurisdiction are challenged. In order to facilitate the use and growth of the extraordinary medium that is the Internet, any effort to deal with regulation or legislation (or standards) should be done in a globally cohesive manner to avoid such a patchwork of compliance. Such global cohesion should be

pursued in a way that establishes a baseline of consistency and fosters innovation, rather than extreme or prohibitive measures.

Best practices for the development of any public policy in the U.S. include the processes embodied in the public private partnership as well as a long tradition of transparency and openness in rule-making. The public private partnership is especially important in the current environment that is so dynamic that new technologies, new products and services, new opportunities, and new threats emerge quickly and require timely coordination and collaboration to address. Legislation and regulation cannot keep pace with the technology – or new threats – so the ability to engage industry and government to address concerns together when necessary is critical to enabling the continued free flow of information. In addition, the industry-led international standards making process allows for the ability to ensure interoperability in new technologies and efforts to address privacy, security, and other operational issues as they arise.

The new technology of the day illustrates how traditional compliance and jurisdictional regimes no longer apply. For example in the era of cloud computing, the determination for "local jurisdiction" is no longer a given. Therefore, we need to look at these issues in new ways that do not lend themselves to protracted and one-size-fits-all rule-making procedures. One example of an iterative and collaborative process could be the Transatlantic Economic Council (TEC). TEC is looking at how the U.S. and the European Union can develop principles to facilitate cross border trade deployment with third parties.

With respect to privacy policy and its impact on the free flow of information on the Internet, TechAmerica reiterates the following points, which were submitted earlier this year with the Department of Commerce.

There are a variety of foreign laws governing how companies collect, use, and disseminate consumer data. Unfortunately this matrix of laws has served as an unnecessary, if not intentional, barrier to effective trade in the digital economy. For example the European Union's data privacy laws, in contrast to the U.S.'s more flexible standards, have proven to be not only burdensome in compliance but also inefficient in implementation.

For example, as defined by the European Data Protection Directive 1995, “personal data” is data that relates to or can identify a living individual. This threshold for protection, based on the mere identity and rooted in the jurisdiction of “collection” contrasts sharply with the privacy laws of some other countries, such as in the U.S., where data use and the risks attributable to misuse is the basis for sector-specific regulations.

To be sure, however, TechAmerica and its member countries applaud the Department’s efforts to mitigate the impact of the EU privacy laws, especially the Department’s role in negotiating the U.S.-EU Safe Harbor Framework. This Framework has facilitated the rapid development of a global Internet economy.

In addition to the U.S.-EU Safe Harbor Framework, the APEC Privacy Framework has been extremely helpful for U.S. technology companies seeking to do business globally. TechAmerica commends the leadership of the Department on the development of the Cross Border Privacy Rules (CBPR). Since the APEC Privacy Framework was endorsed by APEC Ministers in 2005, the Department, in conjunction with other U.S. agencies, has been instrumental in working with its counterparts across APEC economies on a series of Data Privacy Pathfinder projects to develop a system in the APEC region that ensures accountable cross-border flows of personal information for the protection of consumers while facilitating business access to the benefits of electronic commerce. TechAmerica member companies are of the view that the APEC Privacy Framework and the Data Privacy Pathfinder projects represent an important step forward in privacy protection in the 21 APEC economies in which new and flexible approaches to accountability and compliance are envisioned.

Further, notably, we are thankful that the Department has striven to include opportunities for the business community to engage and provide input throughout the APEC CBPR development process. This collaborative effort has been essential given the pace of innovation in electronic commerce. The Pathfinder projects enable a system that allows businesses to create their own CBPRs and consumers to rely upon ‘accountability agents,’ as well as regulators, in the APEC region to make sure businesses are held accountable to their privacy promises. The self-regulatory “trustmark” model has proven

effective in a number of economies to date. As the APEC Privacy Framework demonstrated, a voluntary set of common and broadly-applicable principles can coincide with self-regulation and risk-based approach to compliance obligations and enforcement.

With the APEC success in mind, TechAmerica believes a strong consistent global framework is needed in order for the digital economy to truly flourish. Without such a harmonized framework, technology companies will be forced to make difficult decisions as to whether or not to do business in certain countries for fear of being held civilly or even criminally liable for actions that would otherwise be lawful in the U.S. and elsewhere. Such uncertainty would inevitably lead to less investment and, subsequently, less economic growth. Considering how interconnected the global economy already is, the repercussions of such choices will be felt throughout the world.

The global interconnection is especially true with regard to cloud computing, for example. As cloud computing continues to grow, so, too, will the amount of data crossing national borders. If divergent claims to jurisdiction over user content remain, then it becomes quite difficult for providers to manage their legal obligations and their global technology operations while at the same time protect their consumers.

3. Impact of Restricted Internet Information Flows on Innovation, Trade, and Commerce

There is a wide range of laws and regulations that individual countries have in place regarding the sale of certain types of goods, which impacts the business and compliance costs for industry. For example, the online commerce industry has had to dedicate substantial time and resources to establishing a policy, enforcement, and user education framework that mirrors localized laws and restrictions. These policy enforcement mechanisms require a great deal of human and technological resources that diverge from a business-wide platform globally.

4. The Role of Internet Intermediaries

Many OECD countries have created liability exceptions for internet intermediaries in their e-commerce or copyright laws. These exemptions provide a defense to copyright

infringement to remove secondary liability for their users' content that in some cases require the online service providers to remove infringing materials hosted on their systems or networks after receipt of a valid notice (Notice and Take-down policy), among other requirements. In the US, Section 230 of the Communications Decency Act of 1995 grants immunity from liability for providers and users of an "interactive computer service" who publish information provided by others. The Digital Millennium Copyright Act ("DMCA") creates a conditional "safe harbor" from copyright liability for ISPs for "mere conduit" functions, caching, storing, and information location tools. This also exists in Australian copyright law, as well as in Korean laws, to a more limited and conditional extent. The European Electronic Commerce Directive establishes horizontal limitations from liability for "intermediary information society service providers" when they play a technical role as "mere conduit" and for other activities such as caching and hosting information. However, the OECD refers to specific activities of intermediaries rather than defining categories of service providers, so it does not necessarily cover some of the newer activities of online actors.

In the copyright area, the DMCA provides a workable model for removing restricted content while at the same time protecting Internet service providers ("ISPs") from liability based on certain conditions and encouraging innovation and deployment of Internet services. The DMCA was enacted to implement the copyright treaties negotiated through the World Intellectual Property Organization ("WIPO"), which were carefully crafted to balance the rights and responsibilities of copyright owners, users, and online service providers. Section 512 (a) of the DMCA creates an important bright line limitation on liability, recognizing the role of service providers who function as "mere conduits" and ensuring that "mere conduits" continue to promote the free flow of information.[3] The limitations on liability in the DMCA are not conditioned on a service provider monitoring its service or removing infringing materials when it acts as a "mere conduit." Sections 512 (b), (c) and (d) of the DMCA provide for protections for other critical Internet functions such as caching, storage, hosting and information location tools, and contain obligations to take down materials hosted on the service provider's system or network after receipt of a valid take down notice, among other obligations.

[3] The EU's E-commerce Directive, (2000/31/EC, O.J. L 178 , 17/07/2000), although differing in some respects from the DMCA, importantly also recognizes the principle of service providers acting as "mere conduits" and the bright line limitation on liability that comes with it.

The DMCA also provides important limitations against overly broad injunctive relief. Before ordering an injunction against a service provider, a court must apply four factors, including considering the burden on the provider's network, the magnitude of harm likely to be suffered by the copyright owner if steps are not taken to restrain the infringement, whether the injunction would be technically feasible and effective and not interfere with access to non-infringing materials, and whether there are less burdensome and comparably effective means of preventing access to such materials. *See* DMCA § 512 (j)(2). These injunctive relief protections strike the right balance by helping content owners enforce their copyrights while preserving the limitations of liability provided for in the DMCA.

When the Senate Foreign Relations Committee ratified the WIPO Copyright Treaties and approved the DMCA, it appropriately required that the Executive branch promote the DMCA as the model for other countries to adopt as they update their copyright laws. Other countries have also adopted DMCA-like models, including the EU's E-Commerce Directive and Australia's copyright law. It is critical that U.S. government and other signatories of the WIPO treaties continue to promote the service provider protections embodied in the DMCA as part of any copyright provisions in multilateral or bilateral trade agreements.

Also, Section 230 of the Communications Decency Act of 1995 represents a potential model for countries seeking to encourage responsible voluntary content monitoring without imposing undue liability risks. As the NOI observes, Section 230 has been extremely successful in spurring rapid growth in new Internet services because companies can offer websites, social network, and other services "without worrying about potential liability for information stored on or moving across their networks."[4] The Section 230 principle of facilitating voluntarily efforts to protect customers is one that should be promoted internationally.

Technical issues associated with monitoring, filtering and blocking restricted content must be addressed with care to protect the free flow of information and to avoid unintended consequences for users and service providers, and the security and stability of the Internet.

[4] Free Flow NOI at 60072.

Accordingly, it is important to promote domestic and international policies that – like the DMCA – acknowledge the importance of employing enforcement techniques that are technically feasible and tailored to realistic objectives, and that do not create undue costs or technical constraints for users outside the countries. It is especially important to ensure that blocking policies take into consideration those factors to the extent private sector actors face potential liabilities for compliance failures.

In light of the debate above, the OECD has outlined and is currently deliberating the following principles:[5]

- Determine fair and efficient arrangements for cost sharing for compliance monitoring.
- Undertake risk assessments that evaluate unintended consequences. The consequences of deputizing intermediaries to exercise this capacity on behalf of governments are not clear, with potential unintended consequences.
- Assess the impact of policies on civil liberties and set up safeguards.
- Provide for due process.
- Protect consumers who have obtained content legitimately.
- Reduce the need for Internet intermediaries to have to make subjective assessments of legality.

At the outset of the intermediaries project, it was made clear that the role of intermediaries should be considered alongside all other Internet stakeholders. This implies a need to give due consideration to the complex Internet eco-system and set of inter-relationships within which intermediaries operate, rather than in isolation.

Discussions at the June 16 OECD Workshop on Internet Intermediaries clearly demonstrated that there is no one-size-fits-all approach. And although the discussion at the workshop seemed at times heavily focused on the role of ISPs, key participants and

[5] OECD. (2010, April). Retrieved October 29, 2010, from The Economic and Social Role of Internet Intermediaries.

the broader intermediaries project have emphasized that there are different types of intermediaries, different types of information, different types of solutions and different types of policy approaches. A one-size-fits all solution would very likely lead to unintended economic and social consequences.

All stakeholders, including civil society, industry and indeed Internet users, have a shared responsibility in combating illegal activity on the Internet, so as to ensure the Internet continues as a critical medium for legitimate commerce and speech.

Measures taken by intermediaries to address illegal activity online must be consistent with applicable legal frameworks and foster other legitimate public policy objectives. The overarching goals should be the promotion of innovation, economic development and creativity, while protecting users' legitimate interests.

5. Trade Agreements

The Department of Commerce seeks comment on how bilateral or multilateral trade or other agreements promote the free flow of information over the Internet. To be sure, the technology industry has long supported free trade. TechAmerica believes strongly that trade agreements can and do open up new markets that create new economic opportunities for the industry and the millions of persons the industry employs. Inherent in those opportunities is the ability for information flows to be unimpeded.

Trade Agreements are one powerful tool for promoting the free flow of information over the Internet. Whether in the World Trade Organization or in bilateral or regional free trade agreements, governments can choose to make commitments that will support information flows. The General Agreement on Trade in Services (GATS) provides specifically for the movement of electronic information, goods, and services across borders in its modes of delivery (mode 2) for all services. Combined with telecommunications and value added communications and information technology services, the GATS can be even more fully utilized to bring countries to a more cohesive and harmonized environment for cross border information flows, thereby furthering free flow of information. Trade agreements are an important tool precisely because they are

developed in the context of a legal regime that requires compliance and provides recourse.

Whether in the context of trade agreement negotiation, or other bilateral meetings where regulations are discussed, the focus of U.S. engagement on these issues should be to assimilate best-in-class guidance on criteria for determining when regulations should be applied to a new service or existing service innovation in a national market. Such analysis should take into account gains to be achieved in fostering innovative service deployment. In this regard, we welcome U.S. and EU government objectives for the Transatlantic Economic Council 2010 (TEC) to develop basic principles, for use with third countries, to foster EU and U.S. ICT services sector trade.[6]

TechAmerica suggests that we can take a new approach to trade agreements and evaluate them based on their contribution to technological innovation, thereby furthering previous accomplishments in telecommunications services, value-added service, computer and related services, and e-commerce chapters, as well as the Information Technology Agreement.

6. International Cooperation

The Internet is a complex and ever evolving medium; its complexity and its global, borderless nature make it difficult for policy to keep up with its development and to keep from hampering the use of it. Therefore, international cooperation and dialogue is crucially important to the global free flow of information over the Internet.

It has been helpful for governments, industry, civil society non-governmental organizations (NGOs), and the academic community to convene each of the last five years at the Internet Governance Forum (IGF) came out of the World Summit on the Information Society. The IGF is an evolutionary forum that embodies a global dialogue on an issue of global concern. In its first five years the IGF has addressed various aspect of the Internet under its key themes: access, diversity, security, openness,

[6] *Please see*, Remarks of Deputy Assistant USTR for Europe David Weiner, Transatlantic Economic Council Outreach Session, U.S. Department of Commerce, 26 Oct. 2010 (emphasizing the potential of diverse national non-tariff restrictions to impact cross-border service provision and data flows).

privacy, and Critical Internet Resources. Importantly, the IGF ensures that all stakeholders participate in the sessions and dialogue on equal footing. That parity allows participants to engage in candid exchanges with others on the issues of common concern and have a voice in the preparation for and discussions during the forum. Further, the IGF's non-negotiating framework allows the discussions to be timely and address new developments in the Internet space and focus on the issues rather than the words on a page. Finally, the flexibility of the IGF allows all stakeholders in all geographies to take what they learn from the IGF and implement it in their respective environment.

There are many avenues for international cooperation on Internet issues for specific areas of concern, and those most successful in their impact are those that engage the stakeholders in dialogue on a timely and consistent basis and incorporate economic research in their understanding of the issues at hand.

Conclusion

TechAmerica appreciates this chance to provide its insight, on behalf of its approximately 1,200 members, on the importance of the free flow of information on the Internet. TechAmerica welcomes the opportunity to work further with the Department of Commerce on this vitally important policy issue.