Before the
Department of Commerce
Washington, DC

In re	:	
Global Free Flow of Information on the Internet	:	Docket No. 100921457-0457-01

COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

The Computer & Communications Industry Association ("CCIA") respectfully submits these comments in response to the U.S. Department of Commerce ("DOC"), National Telecommunications and Information Administration ("NTIA"), Notice of Inquiry in the matter of Global Free Flow of Information on the Internet.[1] These comments address: (1) the various worldwide restrictions on the free flow of information over the Internet and their impacts on U.S. firms; (2) CCIA recommendations for combating threats to the free flow of information, both at home and abroad; (3) best practices available to governments to safeguard network security while minimizing restrictions on the free flow of information on the Internet; (4) the significant role of Internet intermediaries and the importance of limiting Internet Service Provider ("ISP") liability to facilitate e-commerce; and (5) the role trade agreements and international cooperation must play in facilitating greater Internet freedom.

CCIA is an international, nonprofit association of computer and communications industry firms. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small

[1] "Global Free Flow of Information on the Internet; Notice of Inquiry," 75 Fed. Reg. 188 (Sept. 29, 2010), pp. 60068-60073.

entrepreneurial firms to some of the largest in the industry. CCIA members employ more than 600,000 workers and generate annual revenues exceeding $200 billion.[2] CCIA is dedicated to preserving full, fair, and open competition throughout our industry, and highly values the ability of the Internet to facilitate the free flow of information and ideas.

I. Introduction

The United States is an information economy, and U.S. companies are leading vendors of information products and services. In this context, information discrimination by other countries fundamentally undermines U.S. economic interests, including the interests of U.S. companies seeking to access foreign markets and those engaged in electronic commerce. Filtering American content and services has the effect of diminishing American competition, and combating it should be a priority.

For too long the U.S. business community has had insufficient support from the U.S. government in responding to other nations' efforts to block and censor the free flow of information. Companies are on the front lines in the battle for Internet freedom, and when confronted with foreign government demands, the governments that are home to these companies must lead in the defense of Internet freedom and free trade principles.

Of course, there are legitimate government concerns over the free flow of information on the Internet. Such concerns and legitimate restrictions are already embodied within the WTO's GATS "general exceptions".[3]

CCIA commends the DOC for taking a step in that direction by raising the increasingly important issues of Internet freedom and online censorship in initiating its Global Free Flow of Information on the Internet proceeding. CCIA urges the DOC to

[2] A complete list of CCIA's members is available online at <http://www.ccianet.org/members>.
[3] *See* GATS Art. XIV.

cooperate with other interested bodies, including the U.S. Department of State, the United States Trade Representative ("USTR"), foreign governments, and multilateral organizations in reviewing impediments to the global free flow of information over the Internet.

Concerns over impediments to the free flow of information over the Internet continue to grow as communications and commerce over the Internet increase. Currently, there are numerous restrictions on the free flow of information over the Internet, and such restrictions harm U.S. trade and commerce, as well as innovation in Internet communications and services. The federal government should take steps to work with foreign governments and multilateral organizations to fully enforce existing trade agreements; close gaps in existing trade agreements in the area of Internet communications and trade; and negotiate stronger rules in future trade agreements to protect e-commerce, limit ISP liability, and stop Internet censorship.

II. Worldwide There Are Numerous Types of Restrictions on the Free Flow of Information on the Internet

A. Approximately 40 Nations Engage in Various Forms of Online Censorship and States are Largely Uncommunicative About Processes or Rationale for Blocking Internet Services

Currently, many countries, to varying degrees, restrict the free flow of information over the Internet. While the rationale for some censorship is known or has been disclosed, governments have typically not communicated processes or reasons for censoring Internet services and content. Nations who have engaged in online censorship include: Afghanistan, Burma, China, Cuba, Egypt, Guatemala, Indonesia, Iran,

Kazakhstan, North Korea, Pakistan, Saudi Arabia, Syria, Tunisia, Turkey, Turkmenistan, Uzbekistan, and Vietnam.

CCIA members report that methods of censorship vary, and include laws, regulations, and court orders that require or forbid various actions. Examples of requirements imposed on Internet services include: blocking access to an entire Internet service or specific keywords, web pages, and domains; requiring Internet search engines to remove search results; and demanding companies take down certain web sites. Additionally, firms are forbidden in some countries from revealing requests made by censorship authorities. Moreover, firms report that they are encouraged to engage in self-censorship by governments through surveillance, monitoring, threats of legal action, and informal methods of intimidation.

With few exceptions, states do not communicate their rationale or processes for blocking or unblocking Internet content or services, and restrictions are not developed in a transparent manner. However, in some instances the rationale for blocking or censoring sites and services has become known.

One such known example is in Turkey. In 2007 the Turkish government passed Law No. 5651, allowing courts to block websites where there is "sufficient suspicion" that a crime has occurred.[4] Crimes on the list include child pornography, gambling, prostitution, and crimes against Ataturk.[5] Crimes against Ataturk include online content deemed to be insulting to Kemal Ataturk, modern Turkey's founder and first president.

---

[4] *International Trade in the Digital Economy: Hearing Before the S. Subcomm. on Int'l Trade, Customs, and Global Competitiveness of the S. Comm. on Fin*., 111th Cong. 3 (2010) (statement of Ed Black, President & CEO, Computer & Communications Industry Association), *available online at* <http://finance.senate.gov/hearings/hearing/?id=2d08f67d-5056-a032-52b8-f7c75d3a3b87>.

[5] Ece Toksaby, *Turkey Reinstates YouTube Ban*, REUTERS, Nov. 3, 2010, *available online at* <http://www.reuters.com/article/idUSTRE6A227C20101103>.

The law resulted in Turkey blocking access to YouTube from May 2008 through October 2010, temporarily lifting the ban, and then recommencing blocking YouTube in November 2010.[6] Additionally, members report that Turkish courts have allowed the government to monitor and block sites such as Amazon, Bing, Google, Hotmail, MSN, and Yahoo for content considered to be blasphemous or anti-Islamic.

In addition to Turkey, CCIA members report that other governments have monitored or blocked sites and content deemed anti-Islamic. Nations with such policies include Pakistan[7] and Afghanistan.[8]

The Chinese government has repeatedly blocked sites and services, including Facebook, Flickr, Foursquare, and Twitter. China blocked Foursquare, a social networking service, ahead of June 4, 2010, in response to a number of users who set their location to Tiananmen Square; users set Tiananmen Square as their location as a way to honor the 1989 Tiananmen Square protests.[9] Additionally, China has singled out U.S. companies, such as Google, for censorship even when Chinese-owned services carry the same, banned content.[10] China has also taken action against U.S. based services in response to specific activities of American firms or the U.S. government. For instance, in response to Congress awarding the Dalai Lama with the Congressional Gold Medal in

---

[6] *Id*.
[7] Ketaki Gokhale and Farhan Sharif, *Pakistan Blocks YouTube, 450 Web Links in Crackdown*, BUSINESSWEEK, May 20, 2010, *available online at* <http://www.businessweek.com/news/2010-05-20/pakistan-blocks-youtube-450-web-links-in-crackdown-update3-.html>.
[8] *See* Sayed Salahuddin, *Afghanistan to Block Some Internet Sites: Minister*, REUTERS, Mar. 4, 2010, *available online at* < http://www.reuters.com/article/idUSTRE62324S20100304>.
[9] Claudine Beaumont, *Foursquare Blocked in China*, THE TELEGRAPH, June 4, 2010, *available online at* <http://www.telegraph.co.uk/technology/socialmedia/7802992/ Foursquare-blocked-in-China.html>.
[10] *See* Simon Elegant, *Chinese Government Attacks Google Over Internet Porn*, TIME, June 22, 2009, *available online at* <http://www.time.com/time/world/article/0,8599,1906133, 00.html>.

October 2007 and the opening of a YouTube Taiwan domain[11], China manipulated its "Great Firewall" to redirect users entering the URL for U.S. search engines to Baidu, the Chinese search engine.[12] Such actions have led one company, GoDaddy, the world's largest domain name registering company, to cease registering websites in China altogether. Specifically, GoDaddy cited intrusive government rules that require registrants of Chinese domain names to provide a color, head-and-shoulder photograph, along with other pieces of business identification.[13] Typically, domain registries only require a registrant's name, address, telephone number, and email address; China is the first government to retroactively seek personal identity information and additional verification and documentation of registrants.[14]

Iran has also blocked online content and services. In the summer of 2009, Iran blocked sites such as Gmail, Twitter, and YouTube in the aftermath of the disputed 2009 election.[15] Democratic opponents of the ruling regime used these services to transmit materials criticizing the regime, and the government's response was to block the websites as part of its crackdown.

Although the rationales for the above instances of online censorship by governments have been disclosed, such disclosure is the exception. Governments that

---

[11] *See* Maggie Shiels, *China Criticised Over YouTube*, BBC, Mar. 25, 2009, *available online at* <http://news.bbc.co.uk/2/hi/technology/7962718.stm>.
[12] Richard Waters, *Google Calls for Challenge to Censorship*, FINANCIAL TIMES, Nov. 15, 2010, *available online at* <http://www.ft.com/cms/s/0/3ab232ec-f0e5-11df-bf4b-00144feab49a.html#axzz174mJTq5m>.
[13] Ellen Nakashima and Cecilia Kang, *In Response to New rules, GoDaddy To Stop Registering Domain Names in China*, THE WASHINGTON POST, Mar. 25, 2010, *available online at* < http://www.washingtonpost.com/wp-dyn/content/article/2010/03/24/AR2010032401543.html>.
[14] *Id*.
[15] *See* Christopher Roads and Loretta Choa, *Iran's Web Spying Aided by Western Technology*, THE WALL STREET JOURNAL, June 22, 2009, *available online at* <http://online.wsj.com/article/SB124562668777335653.html>.

engage in online censorship or blocking or web-based content and services typically do so without communicating the processes by which decisions on censorship are made.

B. Restrictions on Free Flow of Information Favor Domestic Firms to the Detriment of Foreign Firms

Information discrimination represents a classic "non-tariff trade barrier", constitutes an unfair "rule of origin" by filtering out (through a non-transparent process) U.S. originating content such as certain U.S. domains deemed "subversive", and violates the fundamental free trade principle of "national treatment" to U.S. services and service providers. By treating foreign firms differently than domestic firms, offending governments create barriers to market entry that would not otherwise exist, creating advantages for domestic firms and disadvantages for foreign competitors. Such advantages range from intentionally redirecting Internet traffic from foreign sites to domestic sites, to using filtering technology that cause foreign-based services to be degraded for domestic users.

Some governments censor, block, and discriminate against foreign-based web services and content. These actions not only harm the foreign firms, they advantage domestic firms. For instance, in 2007 China blocked U.S. based search engines and redirected users to the leading Chinese search engine, Baidu.[16] Recently, Google endured a standoff in renewing its Internet license in China over the government's censorship policies. Google's policy of redirecting Chinese users to the site's uncensored Hong Kong page led the Chinese government to filter all Google search results through its "Great Wall" monitoring system. As a result, Google's market share fell to 30.9 percent in the first quarter of 2010, down from 35.6 percent in the fourth quarter of 2009; Baidu,

[16] Waters, *supra* note 12.

China's largest search engine, saw its market share increase concurrently from 58.4 percent in Q4 2009 to 64 percent in Q1 2010.[17] As a result of its loss in search market share, Google experienced a drop in advertising revenue in China as advertisers shifted their business to Baidu, allowing Baidu to charge higher rates for advertising.[18]

China has also directly singled out American search sites as purveyors of pornography, even though Chinese services allow users to link to similar content.[19] Numerous other U.S. Internet services, including Blogger, Facebook, Flickr, Twitter, and WordPress have been blocked or severely restricted by the Chinese government, while domestic versions of the same services are permitted to operate, even though they contain similar levels of "offensive" content.[20]

In addition to direct censorship and discrimination against U.S. firms that aids domestic firms, CCIA members report that content filtering by some governments harms the quality of service foreign firms are able to deliver, indirectly advantaging domestic services. For instance, both China and Vietnam filter content and services as transmissions enter the country. This filtering is done at the international gateway through which content and services enter a nation's telecommunications network and become available to users. In filtering the services and content that enter their networks, China and Vietnam ensure that the foreign services available to users are degraded iterations of the service available to users in other markets. As a result, foreign service and content providers must compete with degraded products against non-filtered

---

[17] Mark Lee, *Google Wins China Permit Renewal, Defusing Standoff*, BUSINESSWEEK, July 9, 2010, *available online at* <http://www.businessweek.com/news/2010-07-09/google-wins-china-permit-renewal-defusing-standoff.html>.
[18] *Id*.
[19] *See* Elegant, *supra* note 10.
[20] Jordan Calinoff, *Beijing's Foreign Internet Purge*, FOREIGN POLICY, Jan. 15, 2010, *available online at* <http://www.foreignpolicy.com/articles/2010/01/14/chinas_foreign_internet_purge>.

domestic products, and as a result are disadvantaged in comparison to the domestically based competitors in those countries.

C. Legitimate Restrictions on the Free Flow of Information Are Included Within the World Trade Organization's ("WTO") General Agreement on Trade and Services ("GATS") "General Exceptions"

There are instances in which restrictions on the free flow of information can be legitimate. Restrictions that under the WTO's GATS "general exceptions" are necessary to "protect public morals" or "maintain public order" are legitimate.[21] Additionally, with regards to Internet censorship, there are reasonably available and less disruptive alternatives to blocking or filtering entire Internet services. For example, instead of blocking an entire service, a government may, through a formalized and transparent take-down process, simply request the service provider remove offensive content, or make such content unreachable from IP addresses originating within the country. A government should have a consistent public policy regarding what content it deems offensive. Turkey's list of criminal content, although overreaching, is far preferable to secret ad hoc blacklisting. Additionally, with transparency and due process, governments could by written request direct service providers to block only those web pages with offensive content, rather than blocking the service altogether.

D. The Federal Government Can Assist U.S. Businesses in Gaining Greater Access to New Markets by Closing Gaps in the WTO Framework to Ensure GATS Disciplines Apply to the Internet, and Negotiate New Trade Rules that Protect Internet Trade

The federal government can assist U.S. businesses in gaining greater access to new markets by taking concrete steps to ensure that the rules that govern the next

[21] *See* GATS Art. XIV.

generation of trade agreements reflect the new challenges posed by online government censorship and disruption of the Internet. To this end the government should move to close gaps in the existing WTO framework to ensure all GATS disciplines apply to trade over the Internet. Furthermore, the U.S. should negotiate new rules in bilateral and multilateral trade agreements that advance the unrestricted flow of information over the Internet and increase transparency. The U.S. should also take steps as necessary to re-vitalize the WTO e-commerce working group.

The federal government can also address Internet censorship and its burdens on communications and trade through heightened focus on the issue. USTR should highlight Internet censorship in trade reports. Every year, the USTR conducts the Special 301 review, which assesses our trade relationships with an eye toward intellectual property protection. USTR should establish a Special 301-like process to review and place on a watch list those U.S. trading partners that censor or otherwise restrict Internet services, affecting trade. If it is found that censorship and surveillance unreasonably impairs U.S. business interests, we should reassess and adjust our trade relationships accordingly.

The State Department should actively support the Global Network Initiative ("GNI"). While the State Department already has plans to lend financial support to censorship technology circumvention projects in Internet Restricting Countries, it can move more expeditiously and do more. The federal government should encourage broader American corporate responsibility and participation in GNI. By seeking the participation of industry at home and allies abroad such as the European Union, Congress and the State Department could boost GNI's visibility and effectiveness worldwide.

In the area of intellectual property law the federal government should take steps to encourage international trademark exhaustion globally and to protect parallel import trade. Unfortunately, current trademark exhaustion regimes create barriers to trade in global commerce. Furthermore, the federal government should move to encourage strong first sale doctrine rights and to discourage the misuse of intellectual property, such as that which arose in *Costco v. Omega*.[22]

There are also steps the government can take to address issues that impede the free flow of information in the United States. The U.S. must lead by example when it comes to Internet freedom. We should discourage censorship, restrict intrusive practices such as deep packet inspection, and resist blocking content perceived to be unsavory. Specifically, the government should move to modernize U.S. privacy laws, including the Electronic Communications Protection Act ("ECPA"). On the other hand, recently reported government intentions to expand application of Communications Assistance for Law Enforcement Act ("CALEA") technology mandates to software, applications, and/or personal devices[23] would be counterproductive to promoting the free flow of information on the Internet. Proposals to require Internet communications services to build in back doors for government eavesdropping would create vulnerabilities in secure communications systems. These back doors also make it easier for terrorists and cyber criminals to exploit vulnerabilities.

Failure by the federal government to modernize privacy protections and/or increased government intrusion into the innovation and design of secure

---

[22] *See Omega S.A. v. Costco Wholesale Corp.*, 541 F.3d 982 (9th Cir. 2008), *cert. granted sub nom. Costco Wholesale Corp. v. Omega S.A.*, No. 08-1423 (U.S. cert. granted Apr. 19, 2010).
[23] Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, THE NEW YORK TIMES, Sept. 27, 2010, *available online at* <http://www.nytimes.com/2010/09/27/us/27wiretap.html>.

telecommunications systems and services may force U.S. based customers to procure web-based services from foreign firms, or drive U.S. firms to base operations offshore to escape a cumbersome regulatory regime or inadequate privacy and security protections on U.S. telecommunications networks. Some U.S. data storage firms have already moved servers overseas for these reasons.

The U.S. must prioritize Internet freedom, both at home and abroad. Abroad we must work to highlight and reduce Internet censorship through enforcing existing trade rules and taking appropriate action when those rules are broken. Censorship is a trade barrier and must be treated as such. We must also push for Internet freedom to be part of future trade agreements. Internet freedom must be a priority when U.S. officials visit with foreign leaders. Finally, we must set an example for the world and protect Internet freedom domestically.

III. There are Identifiable Best Practices Governments Can Adopt to Address Network Security and Other Interests While Minimizing Restrictions on the Free Flow of Information

A. Governments Should Work With Internet Service Providers to Collaboratively Address Government Concerns With Regards to Services and Content

As discussed above, there are reasonably available alternatives that allow governments to reach their legitimate objectives of network security without the unnecessary blocking or censorship that invariably disrupts free trade. Reasonable alternatives include asking, through a formalized and transparent take-down process, service providers to take down the specific offensive content, or requesting providers

either block the individual offensive web pages reachable via its service or block access to the offensive content to IP addresses originating within the country.

B. There Are Several Basic Criteria and Best Practices Regarding Transparency that Governments Should Follow to Secure Domestic Network Infrastructure While Minimizing Restrictions on Information Flow to Citizens

In order to secure domestic network infrastructure while minimizing the restrictions on the free flow of information to citizens, there are several best practices governments should implement. First, governments should better enforce existing transparency and due process regimes and ensure those regimes apply to government treatment of the Internet. Second, governments should regularly publish all orders or requests to limit information available over the Internet made to providers of Internet services and content. Presently, such orders are not adequately transparent to the public, and some governments have made it criminal for service providers to make public the government order or request. Third, governments should publish and allow public comment in advance of any measures that impact the provision of Internet information services. Finally, governments should publish the terms of all licenses, including ancillary documents that affect the license terms, for the provision of Internet information services to the extent that a license is required.

IV. Restrictions and Affirmative Burdens on the Free Flow of Information Have Negatively Impacted Innovation, Trade and Commerce

Various restrictions on Internet trade and requirements placed on businesses engaged in trade over the Internet have had negative economic impacts on U.S. firms. CCIA members report that European nations prohibited the sale of unlawful, counterfeit goods over the Internet. These restrictions were extended to include both counterfeit and

genuine products, and prohibited sale over the Internet anywhere in the world if the website offering the product could be accessed from the prohibiting country.

A CCIA member reports it lost a judgment requiring it to pay €35.5 million in damages regarding sales of counterfeit items and €3.05 million for unlawful sales in breach of selective distribution network agreements. Although these judgments were reduced on appeal, they still had negative economic impacts on the company.

Additionally, CCIA member companies incurred over €1.7 million in fines for failure to comply with restrictions on the sale of unlawful goods over the Internet accessible by customers in the restricting country. CCIA members also incurred substantial compliance costs in connection with the injunction on global sales of unlawful and counterfeit goods.

Member companies also report that a European nation placed economically damaging affirmative obligations on Internet retailers. A court in one nation held that Internet retailers and websites that facilitate Internet trade have an affirmative obligation to undertake efforts to prevent the trade of counterfeit goods via their websites.

As discussed above, U.S. search engines lost significant market share and advertising revenue as a result of Chinese censorship. Filtering and censorship of foreign search engines resulted in increased market share and advertising revenue for China's leading search engine, Baidu.

It is clear that requirements and restrictions such as these on providers of Internet services are damaging to the free flow of Internet trade globally and have negatively impacted U.S. firms operating abroad.

V. The Role of Internet Intermediaries

Broadly speaking, limiting ISP liability is instrumental to the promotion of e-commerce. Since the early days of the Internet, Congress has recognized that holding Internet and e-commerce businesses liable for the wrongful conduct of their users would jeopardize the growth of this vital industry and place unreasonable burdens on these companies. Many Internet businesses thrive by helping users connect to each other. For some, facilitating this form of networking is the company's sole purpose. Such networking may be achieved by creating a forum for users to post information or offer sales, such as Craigslist or eBay, by creating search tools to find or gather information, such as Google or Wikipedia, or by acting merely as an information conduit, such as an Internet access provider ("IAP"). Because these businesses connect users to each other, they grow quickly but lack the control that brick-and-mortar businesses have over individual content, due to the extraordinary volume of communications that they make possible. These businesses are, therefore, unusually vulnerable to laws that impose upon them strict liability for the misdeeds of any users. Worse still, legal regimes may impose liability upon companies that make good faith efforts to prevent illegal conduct but which are not always 100% successful.

Congress responded to this problem with two statutes designed to limit Internet businesses' liability for the wrongdoing of others. First, § 230 of the Communications Decency Act provided categorical immunity from non-intellectual property-related liability for user wrongdoing, thus allowing Internet companies to combat undesirable or potentially illegal activity without fear of additional liability. This "preserve[s] the vibrant and competitive free market that presently exists for the Internet and other

interactive computer services."[24] Second, § 512 of the U.S. Digital Millennium Copyright Act (DMCA)[25] provided limitations on remedies available against online intermediaries whose users are implicated in copyright infringement, provided that the service provider complies with a notice and takedown regime specified by statute. Mere liability to rights-holders is not the limit of exposure for Internet and e-commerce providers.

Section 230 particularly has, as the Notice recognizes, "spurred rapid growth in new Internet services and applications by [preventing sites] from worrying about potential liability for information stored on or moving across their networks, thus ensuring a flexible environment for innovation and growth."[26] This growth is a substantial factor in prosperity and job creation; according to a recent report of the National Economic Council, expert estimates indicate that the Internet adds $2 trillion to annual GDP, over $6,500 per person.[27]

Aggressive liability rules impede commercial investment, and Section 230 explicitly recognizes this reality. In CCIA's opinion, the fact that Internet and e-commerce businesses have flourished more readily in the U.S. than in other jurisdictions is directly attributable to the fact that the U.S. Congress has carefully crafted laws to encourage the rapid innovation and entrepreneurial spirit that is critical to Internet companies, establishing certainty and predictability by limiting companies' liability for third party misconduct.

---

[24] 47 U.S.C. § 230(b)(2).
[25] 17 U.S.C. § 512.
[26] 75 Fed. Reg. at 60,072.
[27] Exec. Ofc. Of the President, Nat'l Econ. Council/OSTP, *A Strategy for American Innovation: Driving Towards Sustainable Growth and Quality Jobs*, Sept. 2009, at 5, *available online at* <http://www.whitehouse.gov/administration/eop/nec/StrategyforAmerican Innovation>.

CCIA members thus depend heavily upon protection from unjustified state, federal, and foreign liability claims. The distributed nature of the "long tail" of commerce and communication renders impossible effective *ex ante* policing. This does not mean that online services tolerate misconduct, but rather that online services at best play a reactive role, responding when users and concerned parties raise concerns about particular content.

Unfortunately, limitations on liability are not universal. Even in Member States of the European Union, whose E-Commerce Directive contains a nominally strong safe harbor,[28] U.S. companies *and their executives* have been subjected to civil and criminal liability based entirely on misconduct by third parties on the Internet. In the widely criticized 'Vivi Down' case, corporate executives were criminally prosecuted and convicted when an Italian Internet user posted to the Italian YouTube site a video of students mistreating a disabled classmate, notwithstanding the fact that the video was removed within hours of authorities reporting it to YouTube.[29]

The case *LVMH v. eBay* is another example of asymmetric liability rules for multinational services. In *LVMH*, a French court imposed damages liability on eBay for sales of authentic (non-counterfeited) Louis Vuitton goods by various small businesses and individuals through eBay's site. These sales were legal under U.S. law and were marketed on eBay's U.S.-facing site. The French court found that eBay "amplified" the unlawful marketing of goods by failing to adopt measures to protect activity that was illegal under French law. Many of these goods were not counterfeit under U.S. law.

---

[28] *See* E-commerce Directive, 2000/31/EC of the European Parliament and of the Council of 8 June 2000, arts. 12-15.

[29] Manuela D'Alessandro, *Google Executives Convicted for Italy Autism Video*, REUTERS, Feb. 24, 2010, *available online at* <http://www.reuters.com/article/idUSTRE61N2G520100224>.

Rather, these goods were legitimately manufactured, but their manufacturer had not authorized the sale through eBay. Unlike U.S. law, French law allows a manufacturer to prohibit the sale of its products outside of a "selective distribution network." In short, the French court imposed millions in liability upon a U.S. company for sales of authentic goods that were legal in the U.S. and did not occur in France.[30]

From the perspective of advancing U.S. economic opportunities, such penalties are functionally no different than market barriers. U.S. policy should not accept foreign authorities penalizing U.S. companies for the conduct of foreign citizens who find it economically attractive to do business with services offered by U.S. businesses. The Italian case would not have occurred in the United States, and the result in *LVMH* differed from the U.S. court opinion handed down two weeks later in the *Tiffany v. eBay* case. In *Tiffany*, the court ruled that eBay had no obligation to proactively police its site to prevent the sale of counterfeit Tiffany products by third parties. The court concluded that so long as eBay responded promptly to Tiffany's identification of auctions of counterfeit goods, eBay did not infringe Tiffany's trademarks. [31]

Generally, foreign liability rules must accommodate typical Internet functions such as search indexing, user-generated content, and e-commerce platforms if U.S. information technology and Internet companies are to continue expanding internationally. This includes matters pertaining to intellectual property, including copyright, which will be explored in CCIA's joint response to the Department's recent Notice of Inquiry on copyright matters.[32]

---

[30] Tribunal De Commerce De Paris, June 30, 2008, Geronimi.
[31] *See Tiffany Inc. v. eBay Inc*., 600 F.3d 93 (2d Cir. 2010).
[32] "Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy," 75 Fed. Reg. 61,419 (Oct. 5, 2010). In brief, the lack of a fair use provision or its functional equivalent

VI. Trade Agreements

Trade agreements must promote the free flow of information. Filtering of consumer Internet traffic and content-based site blocking poses a clear threat to U.S. businesses' ability to deliver goods and services to overseas markets. Whether it is bananas or bytes that are stopped at the border, the economic effect on U.S. interests is the same. Regrettably, there seems to be increasing interest amongst governments throughout the world in pursuing policy action in this area, a phenomenon for which our own government unfortunately bears some responsibility.[33] While CCIA maintains the view that the current trading regime already prohibits censorship, filtering, blocking, and other impediments to the free flow of information, this should be more explicit in U.S. trade policy.

U.S. trade policy must also ensure that the providers of Internet infrastructure – the information common carriers – can transmit data traffic without the perpetual risk of unjustified liability. As discussed above, safe harbor laws protecting services for liability for the data they carry must be universally advocated, and consistently enforced.

---

exposes U.S. firms to liability overseas for activities U.S. courts permit. In the Belgian case *Copiepresse*, Ct. First Instance, Brussels, Feb. 15, 2007, Ref. no. 7964, and the German case *Horn*, courts imposed copyright liability on Google for the operation of its search engine in a manner consistent with U.S. law, as established by cases such as *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003) and *Field v. Google Inc*., 412 F. Supp. 2d 1106, 1123 (D. Nev. 2006). In connection with consideration of the U.S.-Peru Free Trade Agreement, Senate Judiciary Committee Chairman Leahy endorsed the concept of including fair use in our free trade agreements on the floor of the Senate, saying "[u]nder our laws, many such new technologies and consumer devices rely, at least in part, on fair use and other limitations and exceptions to the copyright laws. Our trade agreements should promote similar fair use concepts, in order not to stifle the ability of industries relying on emerging technologies to flourish." Cong. Rec. S14,720 (Dec. 4, 2007).

[33] As introduced, the recently offered "Combating Online Infringement and Counterfeits Act" (COICA, S. 3804) authorizes domain seizure and international censorship with little or no process.

Where policies appear to be designed to protect domestic industries from online competition,[34] e-commerce investment will likely move toward less hostile markets. U.S. trading partners should be made to understand the unintended negative effects to their economic development and ability to attract ICT investment. It is no accident that innovation in Internet-connected products and services is concentrated in free societies, and particularly the United States. This fact not only underscores the importance of the free flow of information to our trade policy, it should also help in emphasizing to our trading partners why a free and open Internet is in their economic interest.

Yet regardless of whether penalizing Internet intermediaries in this manner is bad policy for the relevant trading partner, such policies violate long-standing commitments to the free trade system, and must be confronted accordingly.[35] Thus, the Department of Commerce must, along with the U.S. Trade Representative, make the inclusion of proper intermediary immunity a principal element of U.S. trade policy.

At the least, U.S. policy should be to commit to the blueprint established in the Korea-U.S. Free Trade Agreement, under which parties agree to refrain from unnecessary barriers to cross-border information flows. This policy should also be pursued in the WTO Doha Round and the Trans-Pacific Partnership, and a commitment to refrain from unnecessary restrictions on cross-border information flows should become a condition for

---

[34] *See* Scott Lamb, *What Does France Have Against Google?* DER SPIEGEL, Mar. 25, 2005; Elitsa Vucheva, *Sarkozy Offers More Protectionist Europe as French EU Presidency Opens,* Ezilon Infobase, July 1, 2008 *available online at* <http://www.ezilon.com/information/article_1 9578.shtml> *see also* Ian Traynor, *Sarkozy Pledges to Restore Trust in EU as France Takes Over Presidency*, THE GUARDIAN, July 1, 2008, *available online at* < http://www.guardian.co.uk/ world/2008/jul/01/eupresidency.france2>.

[35] *See generally* "Internet Protectionism: How Foreign Courts Have Applied Domestic. Law to the Disadvantage of U.S. Internet and E-commerce Companies," (2009), *available online at* <http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000202/Internet-Protectionism.pdf>.

new entrants to the WTO Agreement. Additionally, the U.S. should encourage progress within the WTO on e-commerce and the free flow of information through a revitalization of the e-commerce working group.

VII. International Cooperation

Inter-governmental bodies like the International Telecommunications Union, Organization for Economic Co-operation and Development ("OECD"), and Asia-Pacific Economic Cooperation are indeed too slow for dealing with new impediments to trade on the Internet. Trade barriers must be quickly addressed and inter-governmental bodies are unequipped to take swift action.

Multi-stakeholder non-governmental organizations ("NGO") can be more nimble, but must all work together if no individual organization (like GNI) is able to develop a critical mass of stakeholders. Currently, companies find themselves in a difficult position; they may fear retaliation from foreign governments if they become active in GNI, but they also risk new statutory penalties from our own Congress if they are seen as complicit in human right violations in Internet restricting countries. Separate from GNI, there is an ad hoc group of U.S. hardware, software and services companies that meets in Washington to discuss many of the issues posed in this notice.

To be effective in this space, any multi-stakeholder organization must have a very broad mission such as "Global Internet Freedom" and include representation from multinationals in the corporate sector, non-commercial NGOs, and expert academics. The multi-stakeholder organization cannot be dominated by a few nation states, as none should be members. But it's also important that companies or NGOs from the same country or even the same hemisphere not dominate the multi-stakeholder organization.

While the Internet Governance Forum can be a valuable resource, it cannot be a ruling body. As discussed above, the OECD and other inter-governmental bodies are unequipped to take swift action to deal with trade barriers; however, such organizations are valuable venues for stakeholders to address issues impacting the Internet and the free flow of information and digital goods and services. Such an opportunity will come in June 2011 when the OECD holds a summit on the Internet economy in Paris.

Private sector support for GNI or any other multi-stakeholder organization has not sufficiently matured, but that's where Congress and the Executive branch can help: by encouraging participation and the development of a critical international mass of companies and NGOs dedicated to Internet freedom and online free trade. GNI already enjoys support from the State Department[36] and key Members of Congress, including Senator Dick Durbin[37] and Congressman Chris Smith[38]; GNI should be able to accelerate articulation of acceptable norms. Such critical mass of international firms will make it much easier to expose and isolate bad actors without fear of individual retaliation, and then smooth the way to more effective diplomacy and trade negotiations to facilitate global free flow of information.

VIII. Conclusion

When we discuss the global free flow of information over the Internet, there are potentially trillions of dollars of U.S. economic activity at stake. There are several steps

---

[36] *See* Secretary of State Hillary Rodham Clinton, *Remarks on Internet Freedom*, Jan. 21, 2010, *available online at* <http://www.state.gov/secretary/rm/2010/01/135519.htm>.
[37] *See* Senator Richard Durban, *Durbin, Coburn Continue to Press Tech Companies on Human Rights Code of Conduct*, Aug. 7, 2009, *available online at* < http://durbin.senate.gov/show Release.cfm?releaseId=316922>.
[38] *See* Representative Christopher Smith, *Smith: Google Should Make Break w/China*, Jan. 13, 2010, *available online at* <http://chrissmith.house.gov/News/DocumentSingle.aspx?Document ID=166611>.

we must take to protect this crucial, job-creating activity so that international markets have increased access to the digital goods and services that U.S. firms provide.

First, the USTR should investigate allegations of information discrimination and Internet censorship, and where appropriate, initiate a trade case. For some trade partners, only the initiation of a trade case may persuade them to open their markets to U.S. goods and services.

Second, digital goods and services should be a central feature of our trade policy. The Administration and Congress should work to implement existing FTAs. Additionally, U.S. trade policy as expressed through new FTAs, the TPP, and the Doha Round should implement strong, enforceable commitments to permit the free flow of information over the Internet and the unfettered exchange of digital goods and services. The U.S. should also work to reinvigorate the WTO e-commerce work group and to establish a commitment to refrain from unnecessary restrictions on the free flow of information and digital goods and services as a requirement for WTO accession. Furthermore, the U.S. should build appropriate safe harbors into our legal trade framework to ensure that providers of online services can transit data without the perpetual risk of unjustified liability.

Finally, we must recognize that Internet freedom starts at home. We must discourage censorship; surveillance; and content blocking, prioritizing, or de-prioritizing whenever possible. If unavoidable, such actions must be time-limited, narrowly tailored, and undertaken in an open and transparent process. Finally, we must eschew attempts to deputize online intermediaries into law enforcement. If the United States cannot maintain a free and open Internet, it is unlikely for other nations will do so.

Respectfully Submitted,

/s/ Ed Black

Ed Black, President & CEO
Catherine Sloan, Vice President Government Relations
Matthew Schruers, Vice President Law & Policy
Phillip Berenbroick, Public Policy & Regulatory Counsel
Computer & Communications Industry Association
900 Seventeenth Street, NW, 11th Floor
Washington, DC 20006
(202) 783-0070

December 6, 2010