

Statement of

Edward J. Black President & CEO of The Computer & Communications Industry Association (CCIA)

Before the

Subcommittee on International Trade, Customs, and Global Competitiveness Committee on Finance U.S. Senate

"International Trade in the Digital Economy"

November 18, 2010

Mr. Chairman, I appreciate the opportunity to testify before the Subcommittee to discuss international trade in the digital economy. I am President and CEO of the Computer & Communications Industry Association (CCIA), an organization that has promoted openness, competition, and free trade for over 35 years.

My testimony focuses on an issue that should be atop the U.S. Government's policy agenda: Internet freedom. We have long argued that the Administration and Congress must prioritize Internet freedom, both at home and abroad. Internet freedom advances our political interest in fostering free and open societies, it advances our economic interest in opening foreign markets for U.S. exports, and it promotes innovation and economic growth at home and abroad. Globally, 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 in the 21st century and must be treated as such. We must also promote Internet freedom via future trade agreements. Finally, we must lead the world by example, and establish domestic policies that protect Internet freedom as well.

The United States is a dynamic information economy, and U.S. companies are leading vendors of information products and services, increasingly doing so online. According to a report by the National Economic Council, estimates indicate that the Internet adds \$2 trillion to annual GDP, over \$6,500 per person.² Total combined business-to-business and business-to-consumer ecommerce shipments, sales, and revenues, as measured by the Commerce Department for 2008, were \$3.8 trillion.³ In this context, discrimination against digital goods and services, or "information discrimination" by other countries fundamentally undermines U.S. economic

¹ A complete list of CCIA's members is available online at http://www.ccianet.org/members.

² 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/StrategyforAmericanInnovation. The Internet also has economic significance to individual Americans. According to Pew Research, 88% of American adults turned to the Internet to cope with and understand the recent economic recession. Internet users increasingly look online for jobs, housing options, and government benefits, bargain-hunting, or improving one's skills or investment strategies. See Lee Rainie & Aaron Smith, Pew Internet & American Life Project, The Internet and the Recession (2009).

³ See U.S. Census Bureau, 2008 E-Stats, at 2 (May 2010). Industries whose product demand is driven by Internet content and services, such as consumer electronics, also make a significant economic contribution. For the same year, 2008, CE industries were responsible for \$1.3 trillion in annual value-added to the U.S. economy. See PriceWaterhouseCoopers, Innovation: U.S. Economic Contribution of Consumer Electronics, at 2 (2008).

interests. Filtering American content and services has the effect of diminishing American competitiveness, and combating it should be a priority.

Currently, many countries, to various degrees, restrict the free flow of information over the Internet. The U.S. business community has had insufficient support from the U.S. Government in responding to other nations' efforts to block, interfere with, and censor the free flow of information, the result of which is that individual companies are unsupported on the front lines in the battle for Internet freedom. This is not a battle that the business community should or can successfully wage alone. When confronted with foreign government demands, the governments that are home to these companies must lead in the defense of Internet freedom and open trade principles.

To ensure that international markets for digital goods and services are adequately open, the Administration must engage 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 and the free flow of information.

The Nature of Internet Restrictions Abroad

CCIA members report that approximately 40 governments now engage in broad-scale online censorship. At times the motivation for censorship is self-evident, or is disclosed, but generally the processes and reasons for censoring Internet services and content are opaque. With few exceptions, states do not attempt to justify blocking or unblocking Internet content or services, and restrictions are not developed in a transparent manner. Known offenders include Afghanistan, Burma, China, Cuba, Egypt, Guatemala, Indonesia, Iran, Kazakhstan, North Korea, Pakistan, Saudi Arabia, Syria, Tunisia, Turkey, Turkmenistan, Uzbekistan, and Vietnam.

Censorship methods vary, but generally consist of (a) legal or regulatory obligations imposed upon intermediary services, (b) blocking and/or filtering executed at the network level through state control or influence over the communications infrastructure, or (c) technology mandates that either hobble user privacy and security, or that force product manufacturers to include intrusive monitoring technology or back-doors.

Examples of legal and regulatory requirements imposed upon Internet services include blocking access to an entire Internet service or specific keywords, web pages, and domains; requiring Internet search engines to disappear search results; and demanding service providers take down certain web sites. Additionally, firms are forbidden in some countries from revealing requests made by censorship authorities.

In 2007, the Turkish government passed Law No. 5651, allowing courts to block websites where there is "sufficient suspicion" that a crime has occurred. Applicable crimes include child pornography, gambling, prostitution, and crimes against Ataturk. Crimes against Ataturk include online content deemed to be insulting to Kemal Ataturk, modern Turkey's founder and first president. 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 2010.⁴ Additionally, 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, including Pakistan and Afghanistan.

Moreover, firms are encouraged to engage in self-censorship by governments through surveillance, monitoring, threats of legal action, and informal methods of intimidation. For example, GoDaddy, the world's largest domain name registering company, ceased registering websites in China altogether, citing intrusive government rules that require registrants of Chinese domain names to provide a color, head-and-shoulder photograph, along with other pieces of personal identification. Typically, domain registries only require a registrant's name, address, telephone number, and email address; China is the first government to retroactively demand additional verification and documentation of registrants.⁵

Blocking at the network level is also troublingly common. 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 as a way to honor the 1989 Tiananmen

⁴ Ece Toksaby, *Turkey Reinstates YouTube Ban*, REUTERS, November 3, 2010, *available online at* http://www.reuters.com/article/idUSTRE6A227C20101103.

⁵ Ellen Nakashima and Cecilia Kang, *In Response to New rules, GoDaddy To Stop Registering Domain Names in China*, THE WASHINGTON POST, March 25, 2010, *available online at* < http://www.washingtonpost.com/wp-dyn/content/article/2010/03/24/AR201003240 1543.html>.

Square protests.⁶ Additionally, China has singled out U.S. companies, such as Google, for censorship even when Chinese-owned services carry the same, banned content.⁷ China has also taken action against U.S.-based services in response to specific activities of American firms or the U.S. Government itself. For instance, in response to Congress awarding the Dalai Lama with the Congressional Gold Medal in October 2007 and the opening of a YouTube Taiwan domain, China manipulated its "Great Firewall" to redirect users entering the URL for U.S. search engines to Baidu, the Chinese search engine.⁸

Iran has also blocked online content and services. In the summer of 2009, Iran blocked sites such as Twitter, YouTube, and Gmail in the aftermath of the disputed 2009 election. As democratic opposition activists were using these services to transmit critical political materials, the government's response was to block the sites and services entirely, as part of a broader crackdown.

We must also take care to monitor standards development in foreign countries, where the process may be closed, and may be driven by government agendas. CCIA has long supported open standards, which provide the foundation for the modern Internet. The U.S. Government should promote open standards development, in a universal, non-country specific manner, and monitor carefully efforts to develop nation-specific standards, particularly those which might advance the interests of a favored domestic company.

Economic Impact of the Global Assault on Internet Freedom

Undoubtedly, the campaign by oppressive regimes against Internet freedom is a direct threat to American values. The free expression and free flow of ideas is a necessary condition for successful governance under democratic principles. Attempts to control the citizenry's access to information must be relegated to the dustbin of history. Government restrictions on content and

⁶ 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.

⁷ 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>.

⁸ Maggie Shiels, *China Criticised Over YouTube*, BBC, March 25, 2009, *available online at* http://news.bbc.co.uk/2/hi/technology/7962718.stm.

⁹ 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.

services are more worthy of "1984" than 2010. Yet this conflict of values – the clash between an open Internet or a closed Internet – poses as dire a threat to our economic interests as it does to our political values. Thus, concerns about information discrimination fall squarely before this Committee, because of the inevitable implications for international trade.

Information discrimination represents a classic "non-tariff trade barrier", constitutes an unfair "rule of origin" by filtering out (though a non-transparent process) U.S. originating content such as certain U.S. domains deemed "subversive", and violates the fundamental free trade principal 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 causes foreign-based services to be degraded for domestic users. This also affects advertisers, who are the direct revenue source for many Internet services. At the same time, restrictions on access to information will reduce demand for computing devices and consumer communications devices, markets in which U.S. businesses have strong positions and strong brands. Information discrimination thus impairs many industries at the heart of the U.S. information technology sector.

As these governments censor, block, and discriminate against foreign-based web services and content, their practices directly or indirectly advantage domestic firms. As noted above, in 2007 China blocked U.S. based search engines and redirected users to the leading Chinese search engine, Baidu. 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, China's largest domestic search engine, saw its market share increase from 58.4 percent to 64 percent over the same period. 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. 11

¹⁰ 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>.

¹¹ *Id*.

China has also directly singled out American search sites as purveyors of pornography, even though Chinese services allow users to link to similar content. ¹² 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. ¹³

In addition to direct censorship and discrimination against U.S. firms that aids domestic firms, CCIA members report that the 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 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 domestic products, and as such are disadvantaged in comparison to the domestically based competitors in those countries.

Refocusing Our Trade Priorities on Digital Goods and Services

The federal government can assist U.S. businesses in gaining greater access to international markets by taking concrete steps to ensure that the rules that govern the next generation of trade agreements reflect the new challenges posed by online government censorship and disruption of the Internet. To this end, the U.S. Government should move to close gaps in the existing WTO framework to ensure all GATS disciplines apply to trade over the Internet. Also, 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.

We must continue promoting signed trade agreements, such as the U.S.-Korea agreement, but we must also modernize our agreements so that they promote the free flow of information. Filtering of consumer Internet traffic and content-based site-blocking poses a clear threat to U.S.

¹² Elegant, *supra* note 6.

¹³ 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.

businesses' ability to deliver goods and services to overseas markets. Whether it is bananas or bytes that are stopped at the border, economic harm to U.S. interests results. How would we react if a foreign government intentionally degraded the quality of a U.S.-manufactured physical good at the border, or even redirected a purchase order to a domestic manufacturer? We must at least insist on transparency and due process for any government attempts to filter or censor. Regrettably, there seems to be increasing interest amongst governments throughout the world in pursuing restrictive policy action in this area, a phenomenon for which our own government unfortunately bears some responsibility. 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. In particularly egregious cases, the U.S. Trade Representative should investigate, and where appropriate, invoke dispute resolution procedures to ensure that our trading partners do not view censorship as exempt from their free trade obligations.

At the outset, our trade policy should minimally 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. These policies should also be pursued in the WTO Doha Round, the Trans-Pacific Partnership (TPP), and as a condition for new entrants to the WTO Agreement. Continuing discussions in the Doha Round and efforts toward the TPP present the most immediate platforms for promoting Internet freedom.

The federal government can also address Internet censorship and its burdens on U.S. communications and trade through elevated focus on the issue. USTR should increase its focus on 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 also be conducting a Special 301-like process to review and place on a watch list those U.S. trading partners that censor or restrict Internet services in a manner that affects trade. If it is found that censorship or surveillance impairs U.S. business interests, we should reassess and adjust our trade relationships accordingly. We also need to readjust our trade focus internally. The Industry Trade Advisory Committee (ITAC) framework still has no independent Internet committee. It is baffling that nearly two decades after the creation of the commercial Internet, our advisory committee structure still lacks separate input from an industry that adds \$2 trillion to GDP.

Liability Rules

A major barrier to international Internet commerce and to our entering new markets is liability. 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 service providers. Due to the extraordinary quantity of data transiting communications networks, these businesses are unusually vulnerable to strict liability for the misdeeds of any users. Unlike many of our international trading partners, Congress responded to this problem with two statutes designed to limit Internet businesses' liability for the wrongdoing of others. First, Section 230 of the Communications Decency Act provided categorical immunity from liability for user misconduct, thus allowing Internet companies to combat undesirable or potentially illegal activity without fear of additional liability. Section 230 provided a foundation for today's highly successful Internet services and applications by establishing a robust limitation on potential liability. Second, Section 512 of the U.S. Digital Millennium Copyright Act (DMCA) 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. The success of Internet and e-commerce businesses in the U.S. must be at least partially attributed to the fact that the U.S. Congress carefully crafted laws which encourage rapid innovation and entrepreneurialism online by establishing certainty and predictability with respect to liability matters.

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 for Internet service providers, 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 Italy, 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. In France, a French court imposed millions of dollars in 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. In both Germany and Belgium, courts have imposed liability on Google for copying necessary to provide search functionality – the same search functionality that U.S. users experience, and that U.S. courts have ruled to be lawful.

Thus, from the perspective of advancing U.S. global economic opportunities, unreasonable liability rules are functionally no different than traditional market barriers. U.S. policy should not accept foreign authorities being able to penalize U.S. companies when foreign nationals find it economically attractive do business with services offered by U.S. businesses. Generally, foreign liability rules must not target typical Internet functions such as user-generated content, search indexing, and e-commerce platforms if U.S. information technology and Internet companies are to continue expanding internationally.

Where policies appear to be designed to protect domestic industries from online competition, 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.

Internet Freedom Starts At Home

We cannot establish global Internet freedom if we do not lead by example, and establish domestic policies that protect Internet freedom. The Obama Administration's Innovation agenda has always emphasized the importance of preserving the American public's nondiscriminatory access to an open Internet here at home. The FCC has developed an extensive record establishing the need for basic net neutrality rules to safeguard against commercial business practices that would impede the free flow of information on broadband Internet access connections in the United States. The U.S. must lead by example when it comes to Internet freedom. In the absence of greater competition for Internet access connections, and lacking wholesale IP interconnection requirements such as those found in Europe and Canada, our own consumers, students,

entrepreneurs, small businesses and nonprofits need some certainty for their own Internet freedom and quality of service. We should discourage censorship, restrict intrusive Internet Access Provider practices such as deep packet inspection, prevent gatekeeping of content by dominant broadband conduit owners and resist temptations to block or de-prioritize legal content perceived to be unsavory.

In terms of domestic government access to private communications, the federal government should move to modernize U.S. privacy laws, including the Electronic Communications Protection Act ("ECPA"). On the other hand, recently reported government efforts to expand application of Communications Assistance for Law Enforcement Act ("CALEA") technology mandates to software, applications, and/or personal devices would be counterproductive to promoting the free flow of information on the Internet. Proposals to require Internet communication services to build in back-doors for government eavesdropping would create vulnerabilities in secure communications systems, making it easier for governments across the globe to further tamp down on the free flow of information, censor content, and block disfavored services. Failure by the federal government to modernize privacy protections and/or increased government intrusion into the innovation and design of secure telecommunications systems and services may force U.S. based customers to procure web-based services from foreign firms instead, or drive U.S. firms to base operations offshore to escape a cumbersome or uncertain regulatory regime.

Conclusion

In conclusion, trillions of dollars in U.S. economic activity may be at stake when we discuss Internet freedom. To protect this crucial job-creating activity, we must take several concrete steps to increase access to digital goods and services markets abroad:

- First, USTR should investigate allegations of information discrimination and Internet censorship, and where appropriate, initiate a trade case. For some of our trading partners, only the initiation of a trade case may persuade them to open their markets to U.S. digital goods and services.
- 2. Second, digital goods and services should be central to our trade policy. Work to implement existing FTAs. In our new FTAs, the TPP, and the Doha Round, we should:

- a. Implement robust, enforceable commitments to permitting the free flow of information, and to the unimpeded exchange of digital goods and services; and
- b. Build appropriate safe harbors into our legal trade framework. U.S. trade policy must ensure that the providers of online services can transmit data traffic without the perpetual risk of unjustified liability.
- 3. Finally, we must recognize that Internet freedom starts at home, and discourage censorship, surveillance, and content blocking or de-prioritizing whenever possible. When it is unavoidable, it must be time-limited, narrowly tailored, and undertaken in an open and transparent process. We must also discourage attempts to deputize or shanghai online intermediaries into law enforcement. If the United States cannot maintain a free and open Internet, it is doubtful that any other nation will do so.

About CCIA

The Computer & Communications Industry Association (CCIA) is dedicated to open markets, open systems, and open networks. CCIA members participate in the information and communications technology industries, ranging from small entrepreneurial firms to the largest in the business. CCIA members employ nearly one million people and generate annual revenues exceeding \$200 billion.