900 17th Street, N.W.
Suite 1100
Washington, DC 20006
Phone: 202.783.0070
Fax: 202.783.0534
Web: www.ccianet.org
Computer & Communications Industry Association

ABSTRACT

Internet Freedom: *How National Policies Have Failed To Protect It And What Can Be Done Now To Build It*

Executive Summary

Over the past decade the Internet has grown into the most efficient tool to spread information and knowledge around the world. The platform provides a level playing field for access to information and it gives disadvantaged people, underrepresented and oppressed groups around the world new opportunities to participate in economic, social, cultural and political activity.

Full access to the Internet and the ability to fully use it for communication and exchanging information, needs to be seen not just as a First Amendment issue in this country, but understood as a human rights issue around the world. Internet freedom is nothing less than freedom of expression in the 21st century.

Openness is inherent in the nature of the Internet, making it both effective and controversial. Totalitarian regimes have depended on tightly controlling the flow of information, both domestically and from the outside world, and they have been increasingly censoring the Internet to maintain their control of information.

Internet freedom has received attention this year as a full-fledged diplomatic issue. While spurred by recent headlines of Google's threat to leave China amid censorship and hacking concerns, the policy debate surrounding Internet freedom involve threats from many countries, which have been brewing for more than a decade.

Today's Internet suffers under the mismatch of a fully globalized technology infrastructure supported by piecemeal speech protection that varies from country to country. The problem grew from years of technological progress without any international framework accompanying that progress.

The lack of global consensus has allowed any foreign state to fill the vacuum with its own interpretation for how to manage this communications tool and to what extent traffic can be monitored, directed or controlled. For too long, Internet Access Providers and tech companies, rather than their governments, have been on the front lines of the battle for Internet openness in foreign countries.

As American Internet companies expand overseas, bringing with them our norms regarding openness and freedom of expression, they are often stymied by foreign rules. Other nations often apply their domestic laws in stifling or protectionist manners, obstructing U.S. businesses' access to markets, and impeding the free flow of information. The United States and other nations, which support freedom, must make clear to these governments that they oppose sabotaging what should be the greatest tool for advancing freedom, knowledge and commerce in the world.

Governments– not companies alone -- must primarily engage with other governments to combat policies that are antithetical to global Internet freedom. And while human rights and freedom of information remain highly visible and critical issues, it will likely take time even for democratic countries to agree on policies for Internet freedom and human rights. In the near term, the United States can start by setting a better example for Internet freedom with its own policies. Internet freedom and policies to ensure it should be a matter of negotiation in future international treaties or trade agreements. In the meantime, the US Trade Representative and State Department can

commit to enforcing existing trade laws, which already contain provisions that could help promote Internet freedom around the world.

Safeguarding the open flow of information and ideas over the Internet should rank at the top of our diplomatic agenda and trade agenda. Allowing Internet freedom to be eroded is one of the biggest omissions and failures of the past decade. But it's not too late to reverse this course and the Obama Administration seems to be paying attention.

WHY IS CENSORSHIP A TRADE ISSUE?

The United States is an information economy, and U.S. companies are leading vendors of information products and services. In this context, information discrimination fundamentally undermines market access for electronic commerce, and combating it should top our trade agenda.

.

- Information discrimination represents a classic "non-tariff trade barrier" (NTB) that we seek to eliminate when opening up foreign markets to U.S. goods. By co-opting U.S. businesses into content filtering, offenders create barriers to market entry that would not otherwise exist.

- Information discrimination constitutes an unfair "rule of origin" by filtering out (through a nontransparent process) U.S.-originating content, for example, certain U.S. domains that protectionist regimes deem to be "subversive."

- Information discrimination also violates the fundamental free trade principle of "national treatment" – it treats U.S. vendors differently by requiring U.S. companies to restrict access to information. Allowing U.S. companies to be perceived as being coerced into lowering their corporate moral standards leads to negative public reaction and even penalties at home.

INTERNET FREEDOM POLICY BREAKDOWNS:

Even as we denounce Internet censorship as too heavy-handed for a modern world, we must examine our own policies that impact Internet freedom. How is it possible that over the past decade we have not protected and advanced the values of open and free communications inherent in American culture and this American innovation? Seemingly small policy choices, which appear benign separately, add up to a national policy that itself may threaten Internet freedom.

1) International Policy Breakdowns

Until the recent actions by the Obama administration, the USTR and State Department failed to make Internet Freedom a human rights issue or a trade issue. Instead, U.S. policies presumed that more trade – even with compromises on censorship and related issues – would eventually lead to democratization. For years, the U.S. did not even raise censorship in the context of a trade concern until the Obama administration finally did last summer when China announced its Green Dam project to require all personal computers be sold with Internet filtering software.

- The USTR issued a report in February 2006 that purported to be a "top-to-bottom" review of U.S.-China trade relations, but did not mention the trade implications of coercing U.S. companies into censorship efforts. Instead the report focused on intellectual property rights infringement.
- The 2007 Country Reports on Human Rights Practices released in March 2008 by the State Department's Bureau of Democracy, Human Rights, and Labor downgraded China on its list of human rights abusers. China, which has been among the most vigorous in its Internet censorship, received a better report on human rights issues than the previous year even though the amount of

surveillance and censorship appeared to have increased.

- The Introduction of the 2008 Country Reports on Human Rights Practices does not mention Internet censorship in its section on developments in Vietnam. Reporters Without Borders ranks Vietnam on its list of Internet Enemies, citing a decree on Internet management and electronic communications that came into force in September 2008 forbidding opposition to the Socialist Republic of Vietnam.

- In May 2008, Iran's Committee in Charge of Determining Unauthorized Sites (CCDUS) expanded its blocking list to include many websites related to women's rights. The Introduction of the 2008 Country Reports on Human Rights Practices discusses women's rights and harassment and abuse of women's rights activists, but does not mention Internet censorship in its section on 2008 developments in Iran.

- Instead of helping tech and telecom companies combat demands of oppressive regimes, Congress responded with proposed legislation -- The Global Internet Freedom Act. GOFA would force U.S. Internet companies to exit nations such as China due to censorship and information demands, despite the positive impact the Internet has on expanding freedom in such countries.

2) Breakdowns In Internet Access Policies

The United States needs to lead by example, but we have not been doing so. Starting with some of the seemingly smaller, more innocuous changes to policy during the last administration, the FCC changed the status of Internet Access Providers and how they are regulated in ways that could pose a threat to Internet freedom and access.

- Internet access in the U.S. is controlled by a telecom (wireline+wireless) and cable duopoly, supplemented somewhat by less robust satellite services. The problems inherent in the lack of competition become evident when Internet Access Providers engage in censorship, as AT&T did when it censored certain anti-Bush lyrics performed by the musical band Pearl Jam on an AT&T webcast of the concert. Having few choices among IAPs also means consumers have little recourse when a company engages in improper filtering or censorship such as when lawful video file-sharing is blocked because it might compete with a cable IAP's own subscription programming.

- Phone companies during the past decade were successful in getting broadband connections classified as "information services"; no common carrier regulation has since been applied to Internet access. And access competition has flatlined. Thus, Americans have no exercisable right to affordable, open Internet access.

- Regulatory and court decisions from 2002-2005 eroded the clarity of legal protections from network level discrimination among end users and messages on the Internet. A content neutral Internet is what has made the Internet a level playing field for similar types of information to compete for attention. Net neutrality is a basic ingredient for freedom and openness of the Internet, but it has instead become a political debate, even in the United States.

- A year ago videos from an inaugural concert online were taken down after copyright violation complaints. Bloggers trying to comment on the presidential debates similarly faced fair use challenges when it came to sharing brief video clips of the debate on their websites.

3) Breakdowns In Policies Allowing Government To Access User Data

We understand there are appealing rationales for various types of censorship and surveillance, such as for security, but there is a cost to freedom nonetheless.

- Rather than deterring censorship, the government seeks greater Internet control for itself. The National Security Agency has allegedly engaged in warrantless wire-tapping of U.S.-based telephone calls.

- During the Bush administration, the Justice Department subpoenaed millions of search results from major U.S. search engines to help demonstrate that regulating sexually explicit Internet content can survive constitutional questions.

- Congress passed the USAPATRIOT Act, which expanded the ways government could obtain and monitor information online.

- Efforts by the executive branch and some in Congress to require long data retention policies clearly for the purpose of government searching private data.

- The federal government encouraged telecom companies to break the law and turn over information on customers without warrants in violation of federal communications law. It did so promising immunity and legal changes later in the Foreign Intelligence Surveillance Act. But such a practice undermines telecom and tech companies' ability to say 'no' to illegal requests of our government that infringe on customers – and make it even harder to refuse similar requests from foreign governments.

- The Washington Post reported Jan. 19, 2010, that the FBI accessed over 2000 phone records by filing requests citing what they later said were phony terrorism emergencies.

It is not that the United States' own electronic surveillance and monitoring initiatives are without some justification, though some are under judicial review. What matters is that such efforts are constitutionally suspect, especially when sweeping in scope, and they undercut U.S. companies' ability to resist heavy-handed regulation by foreign regimes. When being strong-armed by foreign governments U.S. Internet companies can hardly claim handing over user data contradicts American principles of free expression and privacy -- if they are being compelled to do so here.

Of course, warrantless monitoring of telephone calls, burdensome search engine subpoenas, and regulatory power grabs are not to be equated with the systematic oppression in authoritarian states. But quibbling about the order of magnitude of civilian monitoring isn't the sort of leadership that will backstop U.S. Internet companies when they are facing down the Thought Police whether in Beijing or elsewhere.

Moreover, to say that our government coerces Internet companies for noble causes while others do so to repress is missing the point: If our government chooses to lead the fight for Internet freedom, this would also provide political support to U.S. companies. Instead, our government's previous failure to lead, combined with its setting a bad example for the world, has pulled the rug out from companies, and has been a blow to Internet freedom.

If Internet Freedom is lost, it will be because it is the victim of well meaning efforts to address undesirable behavior on the Internet and half-hearted efforts to defend it.

U.S. POLICIES TO PROMOTE INTERNET FREEDOM

We don't want the government to write rules of Internet freedom, but ultimately to lay the groundwork for respecting openness and freedom as a value. To do so, our laws and policies must show leadership by example.

It will be an ongoing, but critical challenge for consumers, Internet-dependent businesses, citizens and our government to put overall Internet freedom ahead of various parochial interests in whatever policy debate of the day they manifest – net neutrality, IP protection, deep packet inspection, privacy, Internet surveillance or censorship. While these issues in Washington are often debated separately, they are all tied to a common ethic of Internet Freedom. We must support measures that promote this common ethic.

Domestic Policies:

- Carefully restrict the use of techniques such as deep packet inspection. Once set up, such practices could be used to do anything from going after alleged copyright infringement to monitoring and cracking down on political dissidents.

- Pass strong net neutrality rules so that no government entity here and no company may control access to the Internet. The US must join other nations in adopting best practices that promote Internet freedom and protecting the open Internet is one of them.

- Promote balanced IP law that does not restrict Internet access as a means of enforcing intellectual property rights.

- Block policy changes that would deputize Internet Access Providers to proactively investigate and enforce laws.

International Policies:

- Enhancing State Department and USTR Coordination: The State Department's Global Internet Freedom Task Force (GIFT) Strategy clearly states that the right to freedom of expression, provided for by both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, applies to communication on the Internet like other forms of communication. GIFT can raise awareness of Internet censorship, but there needs to be a coordinated effort across departments and agencies.

- The USTR must adopt a bolder approach to foreign roadblocks and respond forcefully to protectionist decisions abroad in countries like France instead of negotiating secret trade agreements like the Anti-Counterfeiting Trade Agreement (ACTA).

- Rather than rewarding governments whose courts punish U.S. businesses, we should advocate for common sense Internet laws overseas and focus on protecting the interests of U.S. Internet and e-commerce industries from foreign protectionism.

- We do not seek global governance as many would define it. We want commitment to not regulate the Internet, but simply ensure that access to it is open and not controlled by any country or company.

- The secrecy surrounding deliberations over ACTA threatens the open Internet by perpetuating a norm that secret Internet regulation is acceptable. The policy of ACTA secrecy should be repudiated and discussions about Internet regulation should occur in open, multilateral forums.

- To achieve a minimum level of parity, United States trading partners must provide Internet services safe harbors for user-generated content, permit the use of online materials in relation to providing search functionality, and allow de minimis, nominative uses of trademarks.

- A newly networked world demands a new understanding of trade barriers. There must be a framework to address the issue of free flow of information. This profound issue must be championed primarily on the governmental level, rather than by industry. It must also be addressed multilaterally and bilaterally. The successful result on Green Dam was due in part to the coordination between the U.S. and allies like the E.U. and Japan. Our government and others committed to the free flow of information need to come up with rules of the road for this new, networked world, perhaps through an International Internet Freedom Agreement.

CONCLUSION

U.S. officials and human rights activists around the world have shown a growing understanding of the power of the Internet to be either the greatest tool for freedom of speech and participation in a democracy, or the most efficient tool ever to repress speech and maintain a closed society.

The battle is larger than headlines like the showdown between a search engine and the Chinese government. Recent events, however, should be a wake up call to fight for Internet freedom – for protecting that openness and access for citizens around the world. As we consider various domestic and international policies, attention should be paid to whether they support or diminish Internet freedom. Perhaps the greatest threat to Internet freedom is death by a thousand cuts – not a sudden fatal blow, but a chipping away of the openness as everyone from the federal government to local sheriffs ask to monitor or surveil Internet users.

If the Internet is to fulfill its potential as the printing press of the Digital Age, neither a government nor an IAP should act as a gatekeeper, quashing access at its whim. Governments that censor may not easily change their ways, but they need to be made to understand the depth of the U.S. commitment to Internet freedom. We must elevate this issue to the top of our diplomatic and trade agendas, thereby helping other nations understand our commitment to curbing threats to Internet freedom in whatever form they manifest.