Internet Freedom: A Background Paper

Shanthi Kalathil

October 2010

As use of the Internet has grown exponentially around the world, so too have concerns about its defining attribute as a free and open means of communication. Around the world, countries, companies and citizens are grappling with thorny issues of free expression, censorship and trust. With starkly different visions for the Internet developing, this era presents challenges—and also opportunities—for those who wish to ensure the Internet remains a backbone of liberty and economic growth.

U.S. officials have made clear their vision for the Internet's future. President Obama, in a speech before the UN General Assembly, said that the U.S. is committed to promoting new communication tools, "so that people are empowered to connect with one another and, in repressive societies, to do so with security. We will support a free and open Internet, so individuals have the information to make up their own minds." His words were reinforced by FCC Chairman Julius Genachowski: "It is essential that we preserve the open Internet and stand firmly behind the right of all people to connect with one another and to exchange ideas freely and without fear."[1]

Indeed, a free, widely accessible Internet stands at the heart of both global communication and global commerce. Internet freedom enables dialogue and direct diplomacy between people and civilizations, facilitating the exchange of ideas and culture while bolstering trade and economic growth. Conversely, censorship and other blockages stifle both expression and innovation. When arbitrary rules privilege some and not others, the investment climate suffers. Nor can access be expanded if end users have no trust in the network.

However, making reality live up to aspirations for Internet freedom can prove difficult. Numerous global initiatives—spearheaded by governments, private sector and civil society—are attempting to enshrine the norms, principles and standards that will ensure the Internet remains a public space for free expression. At the same time, other norms are fast arising—particularly those defined by authoritarian countries that wish to splinter the Internet into independently controlled fiefdoms. Even as Internet access has expanded around the world, many

1. John Eggerton, "Genachowski, Obama on Same Open Net Page," *Broadcasting & Cable*, September 23, 2010.

governments are attempting to control, regulate and censor the Internet in all its forms: blogs, mobile communication, social media, etc. Such governments have devoted vast resources to shaping the Internet's development within their own borders, and they are now seeking to shape the Internet outside their borders as well. Indeed, Internet experts are worried that national governments of all stripes will increasingly seek to extend their regulatory authority over the global Internet, culminating in a balkanized Internet with limited interoperability.

Hence, the next few years present a distinct window of opportunity to elevate the principles of the free exchange of ideas, knowledge and commerce on the Internet. While U.S. leadership within this window is vital, a global effort is necessary to ensure that these norms become a standard part of the Internet's supporting architecture.

This background paper will describe different concepts of Internet freedom, discuss examples where conflicting interests come into play and explain some of the current international policy, private sector and civil society approaches toward the issue. It does not seek to endorse particular initiatives or policy solutions, but will frame several questions as a jumping-off point for further discussion.

Aspects of Internet Freedom

Internet freedom is perhaps more easy to define by what it is not than by what it is. Examples from around the world are usually cited to define what an attack on Internet freedom looks like (several of which are enumerated in the subsequent section). As a result, while many groups do make the effort to outline the components of Internet freedom, there is little common consensus on a precise normative definition. Rather than attempting such a definition here, this section will examine the various aspects of Internet freedom that are relevant for IDEA.

Because the Internet inherently generates knowledge and value from end users, rather than centralized gatekeepers, freedom of use and access is to some extent inherent in the design of the Internet. Accordingly, the policy framework already governing the Internet has developed in such a way to enhance competition, innovation, free expression and trust, with minimal government intervention.

Moreover, there is already a strong level of global consensus about the fundamentals underlying Internet freedom, in the shape of the core goals and principles to govern access and use of public networks that are crucial to the public interest. For instance, one strongly recognized principle implies freedom of access and freedom to publish. This includes freedom of access to anyone who wants to connect to the public Internet across all platforms (wired, wireless, satellite, etc.). Meanwhile, nondiscrimination principles have long recognized that public networks are an open conduit for content, whether opinions voiced in phone calls or

data transmitted on the network. In this sense, Internet freedom can be construed to be implicit within many of the principles carried over from older communication regimes.

That said, Internet freedom is perhaps most commonly situated within a political context. This aspect of Internet freedom generally emphasizes freedom of expression and human rights, in particular the idea that offline human rights and freedoms should also apply on the Internet. This concept is inherent in the pronouncements of various U.S. officials who have extolled the principle of Internet freedom over the last couple of years. Secretary of State Hillary Clinton summed up this perspective when she said "the Internet is a network that magnifies the power and potential of all others. And that's why we believe it's critical that its users are assured certain basic freedoms. Freedom of expression is first among them."[2]

Several groups are seeking consensus around this dimension of Internet freedom. The Internet Rights and Principles Coalition, a dynamic coalition spawned by the Internet Governance Forum, is seeking to apply the Universal Declaration of Human Rights to Internet governance and policy issues. Some civil society groups focus more narrowly on the concepts of free expressions and privacy as crucial to a free and open Internet, while others monitor the activities of governments worldwide on issues such as censorship, privacy and so on. All of these groups, to one extent or another, affirm that freely accessible information and communication, alongside the right to privacy, is crucial for the further development of open, democratic societies.

There is another aspect to Internet freedom that, while not as commonly discussed, is growing in relevance. This is the economic aspect of Internet freedom, which links the importance of free and open networks with economic growth, trade and favorable business environments. As Secretary Clinton pointed out in her Internet freedom speech of 2010, principles like information freedom are simultaneously connected to core U.S. values and good for business. Countries that censor news and information, she said, should recognize that from an economic standpoint, there is no distinction between censoring political speech and commercial speech.[3] Indeed, she and others have pointed out that countries that routinely filter and monitor content may see an adverse effect on investment, entrepreneurship and new product innovation.

According to this perspective, when governments pursue censorship in a way that favors domestic companies, it counters basic international trade principles such as nondiscrimination and the maintenance of a level playing field. Because of this discrimination, local companies gain a business advantage and domestic con-

2. Hillary Clinton, "Remarks on Internet Freedom," (Speech, Newseum, Washington, D.C., January 10, 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm.

3. Ibid.

sumers lose the ability to choose between providers. It is possible such concerns can be addressed through trade agreements, trade tools and trade diplomacy.[4]

Discussions of Internet freedom are not limited to the U.S. and the rest of the developed world. Regional meetings of the Internet Governance Forum in 2010, including the Asia Pacific Regional Internet Governance Forum, the Central Africa Internet Governance Forum, the East Africa Internet Governance Forum, the West Africa Internet Governance Forum, the European Dialogue on Internet Governance and the Latin America and Caribbean Internet Governance Forum, attributed tremendous importance to the concept of an open and free Internet. According to a report from these meetings, while regional variation exists, there is a large degree of international consensus over the so-called ideal form of the Internet—"namely, an open but secure Internet that is accessible and empowering for all."[5]

Examples of Threats to Internet Freedom

Most of the discussions on Internet freedom have centered on the actions by some governments to censor, filter or demand data on end users. Such actions, particularly in the context of an authoritarian political context, can not only have a chilling effect on free expression and commerce, but can put the livelihoods and even the lives of Internet users at risk.

Freedom House, which surveyed freedom on the Internet in 2007 and 2008, notes that several governments, particularly in authoritarian countries, are creating pervasive, sophisticated and multilayered systems of censorship that limit the type of information citizens can access, create or transmit via the Internet and mobile phones. Even in less restrictive environments, governments have devised more subtle methods to manipulate online discussion, while deploying vague security laws to harass and intimidate Internet users. Much of this results in circumscribed speech and activity on the Internet, as many in these circumstances resort to self-censorship to avoid crossing red lines. "On the whole, threats to Internet freedom are growing and have become more diverse, both in the array of countries that impose restrictions and in the range of methods employed," according to the Freedom House report.[6]

4. Alan Davidson, Statement Before the Congressional-Executive Commission on China Hearing on "Google and Internet Control in China: A Nexus Between Human Rights and Trade?" (March 24, 2010), http://www.cecc.gov/pages/hearings/2010/20100324/davidsonTestimony.pdf.

5. Internet Rights and Principles Coalition, "Human Rights at the 2010 Regional IGFS: A Global Report, September 2010," http://internetrightsandprinciples.org/node/361.

6. Freedom House, "Freedom on the Net: A Global Assessment of Internet and Digital Media," (2009), http://www.freedomhouse.org/template.cfm?page=384&key=194&parent=19&report=79.

Governments have several ways of filtering and monitoring the Internet:

- Key-word list blocking: Any Internet packets featuring certain keywords are dropped.
- Domain name system poisoning: A user's request is intentionally misdirected to another IP address.
- IP blocking: All packets going to or from targeted IP addresses are blocked.
- Bandwidth throttling: Data volume is kept low to limit the amount of traffic that can be sent over the Internet.
- Traffic classification: More sophisticated than IP blocking, this halts any file sent through a certain type of protocol, such as FTP.
- Shallow packet inspection: Packets are blocked based on their content, making broad generalities about traffic based on the packet header.
- Packet fingerprinting: More refined than shallow packet inspection, fingerprinting looks not only at packet header but at length, frequency of transmission, and other characteristics.
- Deep packet inspection: The most refined method for blocking Internet traffic, it examines not only a packet's header but its payload, giving the ability to filter packets at a surgical level.[7]

A few country examples illustrate more vividly the implications of these filtering and monitoring techniques. Iran, for instance, has approximately 23 million Internet users, while its filtering and monitoring system is one of the most extensive in the world. The government also restricts access by limiting the speed of Internet access that ISPs can provide to households and public access sites, making it one of the only countries in the world to do so. This makes downloading multimedia content extremely difficult and blocks off entire portions of the global Internet to the Iranian population.[8]

Iranian bloggers are required to obtain licenses, and content is subject to approval by government ministries. Despite this, the Iranian blogosphere is particularly vibrant. Real-time microblogging, such as through Twitter, has been an important mode of political communication both within Iran and between Iran

7. Casey L. Addis and Thomas Lump, "U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology" (Washington, D.C.: Congressional Research Service, 2010).

8. Ibid.

and the outside world (although some have questioned its ultimate effectiveness in spurring political change). After disputed 2009 elections in Iran, Internet activists and bloggers were detained at an increasing rate, leading human rights monitors outside the country to suspect that the country's Internet monitoring system was even more sophisticated than previously supposed.[9]

China is another country that has frequently been highlighted in discussions about threats to Internet freedom. With the world's largest number of Internet users (roughly 330 million), China's actions online can reverberate globally. The government controls Internet content and expression through a number of means, including blocking, filtering, registering of websites, crackdowns on Internet service providers and encouragement of self-censorship. It also proactively uses the Internet to reinforce state goals and has famously employed thousands to express pro-government views online.

The interaction between U.S. technology companies and China's Internet policies has undergone close scrutiny in recent years. Some human rights activists and U.S. policymakers say that U.S. technology companies have sold services and technologies to China that help the government halt free speech online and identify Internet users. The companies, in turn, have responded that they are abiding by the laws of the countries in which they operate and that they do not actively cooperate or collaborate with the Chinese government in aiding censorship and monitoring.[10]

The recent experiences of Google in China illustrate how Internet freedom issues exist within a complex juncture between governments, companies and civil society. Google launched its Chinese search engine, Google.cn, in January 2006; it became the second most popular search engine in China, behind local search engine Baidu. Google.cn's search results were censored, in compliance with Chinese government requests; Baidu, as far as evidence can determine, has always complied with Chinese government requests. In December 2009, Google detected a highly sophisticated attack, originating from China, on its corporate infrastructure. After a subsequent investigation showed that several other companies were also targeted, and that malware had also opened up email users (and in particular known democracy activists) to surveillance by third parties, Google announced it would stop censoring results in China and redirect users of its Google.cn search engine to the uncensored Hong Kong version.

In this particular instance, there are few clear winners. One that seems to emerge, however, is Chinese search engine Baidu, which along with nearly all other Chinese companies is assumed to routinely comply with Chinese government monitoring and surveillance demands. Many Chinese companies are not

9. Ibid.

10. Ibid.

transparent about how often and in what manner they shape Internet traffic, although many openly say that they cooperate willingly with the Chinese government on these issues. Unlike international companies, which are subject to various forms of public pressure, domestic Chinese companies are largely absent this type of scrutiny, and can benefit when large international players run afoul of government policies. Because of this and other examples, some civil society and industry groups are pushing for a trade-related approach to Internet freedom.

Not all such examples occur in authoritarian countries. India, for instance, joined such countries as Saudi Arabia and the U.A.E. in demanding that Research In Motion (RIM), creator of the BlackBerry, provide the government access to encrypted information sent over its devices, in what the Indian government called an effort to combat terrorism. India has threatened to ban the use of BlackBerry devices unless RIM agrees to grant the government greater access. India is also seeking greater access to encrypted data sent over other services like Skype and Gmail, as well as virtual private networks. Some business analysts and domestic companies say such a development could seriously dampen the environment for foreign investors, who might think twice about investing in India if data is perceived to be at risk.[11] The Indian government, however, maintains that pursuing national security through such endeavors is both legitimate and necessary. In this, it is joined by a number of other national governments. Balancing the competing demands of security and openness is a theme that runs throughout many discussions of Internet freedom.

Western governments have also held technology companies responsible for content uploaded by users. In February of this year [2010], an Italian court found three current and former Google executives guilty of privacy violations after a group of Italian students uploaded a video of themselves bullying a classmate. Google plans to appeal the decision.

Many of these examples raise the issue of intermediary liability, in which governments or other litigants hold telecom and technology companies (intermediaries) liable for unlawful or otherwise harmful content created by users of their services. In some countries, such as the U.S., intermediaries are generally protected from liability for the actions of third parties. However, in many countries around the world, and in particular those countries that tend to censor/monitor the Internet, intermediaries are not protected from such liability (witness the Italy example mentioned above). This has a chilling effect on Internet freedom, as intermediaries tend to err on the side of caution by discouraging the free flow of information. Because of this, civil liberties NGOs and other freedom of expression-related orga-

11. S. Ramadorai, "Don't Disconnect India," *Hindustan Times*, September 21, 2010, http://www.hindustantimes.com/News-Feed/Columns/Don-t-disconnect-India/Article1-603075.aspx.

nizations tend to side with the companies in lobbying for enhanced intermediary protection. Some argue that enhanced intermediary protection globally could help support Internet freedom.[12]

One last example from China shows how a concerted effort by the U.S. government, civil society (both within and outside China) and industry can be effective when addressing challenges to Internet freedom. In 2009 the Chinese Ministry of Industry and Information Technology (MIIT) mandated that later that year all computers sold in China would need to be pre-installed with ostensible child-protection software, called Green Dam-Youth Escort. Studies of Green Dam showed that the software also censored political and religious content and logged user activity. Because the software also had programming flaws that increased user vulnerability to attack and violated the intellectual property rights of a U.S. company's product, it was also easily opposed by U.S. industry. Chinese civil society, too, opposed the software; not only was Green Dam ridiculed for being a clumsy attempt at suppressing free speech and consumer choice, but it was held up to be an example of crony capitalism because the software company's founders were perceived to have relied on government ties for their success. In the face of this united opposition, the MIIT backed down.[13]

The Green Dam example demonstrates that concerted opposition can thwart censorship and surveillance plans by authoritarian governments. It is also something of a special case, as it is rare for this particular blend of circumstances to occur. Nonetheless, it provides an interesting illustration of how different stakeholders with differing rationales for action can come together to successfully uphold Internet freedom.

Current Initiatives

Because there are so many current initiatives addressing various aspects of Internet freedom, the following summary represents a mere sampling of the more prominent activities. They are divided up below into four broad categories: intergovernmental, U.S. government, civil society and private sector. Despite the rough categorization, many initiatives naturally span more than one of these categories.

Intergovernmental Initiatives

Intergovernmental institutions have been active in both Internet governance and the more specific issue of Internet freedom. In most cases, however, there

12. Center for Democracy and Technology, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," April 2010, http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability (2010).pdf.

13. Rebecca MacKinnon, "After the Green Dam Victory," *CSIS Freeman Report*, June/July 2009, http://csis.org/files/publication/fr09n0607.pdf.

has been more action on defining and debating norms and principles, and less on concrete initiatives.

There are several UN-led and UN-related initiatives on Internet freedom. The UN Special Rapporteur for Human Rights, Frank La Rue, is preparing a report to present to the UN Human Rights Council on Internet freedom. The consultative process has been supported by the Swedish and French governments, and it is getting some buy-in from countries around the world, including those in the Middle East and Latin America. If accepted, its sponsors hope it could lead to a UN resolution.

Perhaps the most prominent UN offshoot is the Internet Governance Forum (IGF), a multistakeholder forum for policy dialogue on issues of Internet governance. The establishment of the IGF was formally announced by the United Nations Secretary-General in July 2006, and it has held annual meetings (along with related activities). The IGF addresses public policy issues related to Internet governance, facilitates discourse between organizations engaged in Internet governance, and helps promulgate best practices and builds stakeholder capacity, particularly those from developing countries. At its most recent meeting in Vilnius in September 2010, the IGF addressed several issues relating to Internet freedom.

One of the "dynamic coalitions" spawned by the IGF is the Internet Rights and Principles Dynamic Coalition, formed by civil society groups and other institutions that want to establish an Internet governance regime founded on human rights. The Internet Rights and Principles group is more of a distributed, collective effort than an organized movement, and its main contribution is to flesh out a conceptual and practical framework for work on this issue. Another related group, the Dynamic Coalition on Freedom of Expression and Freedom of the Media, has similar goals but takes a more narrow focus.

Regional bodies have also undertaken some effort in this area. The Council of Europe created an Ad Hoc Committee on E-Democracy to investigate the use of ICT to strengthen democratic institutions and the democratic process. The EU and Council of Europe also presented a proposed "global Internet treaty" at the IGF meeting in September 2010, outlining 12 principles of Internet governance, including upholding openness, interoperability and the rights to freedom of expression and association. According to its drafters, it is based on the 1967 Space Treaty, which decreed that space exploration should be conducted for the good of all nations. Analysts deem it a response to increasing pressure from national governments to regulate and balkanize the Internet.[14]

14. Mark Ballard, "Europe Calls for Global Internet Treaty," ComputerWeekly.com, September 17, 2010, http://www.computerweekly.com/Articles/2010/09/17/242901/Europe-calls-for-global-internet-treaty.htm.

U.S. Government Initiatives

Over the last several the years various initiatives have emerged from the executive and legislative branches of the U.S. Government. These initiatives appear to be in a process of ramping up.

Secretary of State Hillary Clinton's January 2010 speech on Internet freedom set the stage for renewed vigor within the State Department on Internet freedom issues. The State Department's Netfreedom Task Force (formerly the Global Internet Freedom Task Force), chaired by Undersecretary Bob Hormats and Undersecretary Maria Otero, serves as a policy coordinating body within the State Department and includes participation from regional bureaus, public affairs and the Office of the Legal Adviser. The task force operates according to three core principles: advancing Internet freedom through expanded access, monitoring Internet freedom and responding to threats to Internet freedom. The State Department also funds various Internet freedom activities through the Bureau of Democracy, Human Rights and Labor and the United States Agency for International Development.

The Commerce Department has convened an Internet Policy Task Force comprised of staff from the National Telecommunications and Information Administration, the International Trade Administration, the National Institute of Standards and Technology and the Patent and Trademark Office. The Task Force is now seeking public comment on the extent to which governments may be restricting information and inhibiting innovation and economic growth for U.S. companies. Commerce Secretary Gary Locke has framed the issue of Internet freedom in trade terms, noting that preserving the free flow of information online supports the President's National Export Initiative and that one goal is to remove barriers that prevent U.S. companies from getting free and fair access to foreign markets. After reviewing comments, the Task Force will submit a report that will contribute to U.S. policy on these issues.

The U.S. Trade Representative (USTR) has been interacting with companies and civil society organizations on the issue of free trade and Internet freedom. Some civil society organizations would like to see the USTR make provisions to protect freedom of expression online in future U.S. trade agreements, similar to labor protections, although it is unclear to what extent this idea has gained traction. One bill introduced in Congress in 2010, the One Global Internet Act, would first require the federal government to identify "priority" Internet concerns overseas and then require the USTR to begin an investigation under the 1974 Trade Act, which authorizes sanctions and retaliatory actions. Some trade scholars, however, are skeptical about the effectiveness of this approach.

In addition to this act, the most notable piece of legislation to emerge from the U.S. Congress on this issue is HR 2271 [111th], the Global Online Freedom Act, introduced by Representative Chris Smith (R-NJ) in 2007. This legislation would create an Office of Global Internet Freedom at the State Department and would also mandate that U.S. Internet companies take action to combat censorship and protect privacy or be subject to criminal or civil prosecution. The legislation has been supported by some in the House (including then Minority Leader Nancy Pelosi, (D-CA)) but opposed by telecommunications and Internet companies, the U.S. Department of Justice and some civil liberties group, who argue that some of the provisions of the bill are unworkable and likely counterproductive. It has not come to a vote.

Civil Society

Many civil society groups worldwide have engaged the subject of Internet freedom, with most of them addressing the issue within the framework of human rights, freedom of expression and privacy. The major human rights organizations, such as Amnesty International and Human Rights Watch, have all worked on Internet freedom in some capacity, while specialized organizations, such as Reporters Without Borders, the Committee to Protect Journalists, the World Press Freedom Committee, Freedom House and others have dedicated particular initiatives to Internet freedom.

One initiative that has done much to clarify the state of Internet freedom around the world is the Open Net Initiative, a collaborative partnership between the Citizen Lab at the Munk Centre for International Studies at the University of Toronto, the Berkman Center for Internet and Society at Harvard University and the SecDev Group (Ottawa). It aims to investigate, expose and analyze Internet filtering and surveillance in order to inform better public policy and advocacy work. The Open Net Initiative has done much to clarify the scope and scale of global Internet filtering.

In recent years, the NGO community has begun to push beyond research and advocacy on Internet freedom to engage concretely with the private sector and policymakers. For instance, the Global Network Initiative (GNI) was formed to provide practical solutions to complex issues of Internet freedom, and counts among its members companies, civil society organizations (including human rights and press freedom groups), investors and academics. Created by a number of key companies and human rights organizations (including Google, Yahoo and Microsoft as its founding members), the GNI describes as its core features a foundation upon international human rights standards, a multistakeholder approach and global applicability. The GNI advocates thorough human rights due diligence by technology and telecom companies, as well as independent assessment of individual companies' human rights impacts.

In fact, many human rights organizations have called for transparency in company-government relations, the implementation of human rights assessments by technology and telecommunications companies before entering new markets, and third party independent assessment of the human rights impact of companies' activities. The last issue in particular has met with some resistance by companies, who argue that a strictly voluntary approach is less burdensome and raises fewer legal concerns about confidentiality. The GNI maintains that the independent assessment process is crucial to credibility and that many legal concerns (including confidentiality requirements, trade secrets, attorney-client privilege and legal constraints) have been addressed in the design of the assessment process. Perhaps due to its middle-of-the-road approach, the GNI has failed to attract some human rights groups (who deem it too "soft") and many technology companies (who believe its approach too binding and/or intrusive).

Private Sector

Many in the private sector have argued that it is easiest for companies to address the Internet freedom issue from a trade perspective. According to the Computer and Communications Industry Association, censorship, or "information discrimination" as it calls it, can be considered a classic "nontariff trade barrier" that is often targeted for elimination when opening up foreign markets to U.S. goods. When governments force U.S. companies to filter content, the argument goes, this creates a barrier to market entry that otherwise would not exist. It may also constitute an unfair "rule of origin" by nontransparently filtering out certain U.S. or other domains.[15]

This trade-centric argument has also been supported by some within civil society. The First Amendment Coalition also supports using trade rules to enforce Internet freedom, arguing that, for instance, nonlocally based websites suffer performance degradation within China, forcing international companies to locate physically within the country—essentially making China's firewall a trade barrier. The First Amendment Coalition has submitted a report to the USTR, and consultations regarding the effectiveness of bringing a WTO case seem to be ongoing. The USTR has said in the past that trying to resolve the issue through bilateral forums such as the U.S.-China Joint Commission on Commerce and Trade (JCCT) might be preferable to what could be a multiyear battle in the WTO.

15. Computer and Communications Industry Association, "Internet Freedom: How National Policies Have Failed to Protect It And What Can Be Done Now To Build It," http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000315/InternetFreedomwh.pdf.

Some individual companies have also committed, in various forms and to varying degrees, to increased human rights-related activity and transparency with respect to government requests for censorship. Yahoo, which suffered negative publicity when it complied with a Chinese government request to turn over identifying information about dissidents, has since led the field in Internet freedom-related corporate initiatives. Yahoo conducts human rights impact assessments in order to understand the human rights implications of their business decisions, especially when entering a new market or launching a new product. The company has worked with the Laogai Research Foundation to create the Yahoo Human Rights Fund to provide humanitarian and legal support to political dissidents imprisoned for expressing views online. Yahoo has also created a Business and Human Rights Program to coordinate and lead the company's efforts to protect and promote free expression and privacy.

Google has also sought to implement various transparency initiatives relating to government censorship of its services. The company now provides an interactive map that displays the number of government inquiries for information about users and requests for Google to take down or censor content. Its traffic graphs also provide information about traffic to Google services around the world, including historic traffic patterns for a given country/region and service. Google says that by illustrating outages, the traffic tool helps display disruptions in the free flow of information.

Going Forward: Questions for Discussion

Many agree broadly that governments, companies and civil society must work together to devise and implement effective approaches to advance Internet freedom. However, for each initiative proposed above, there is ongoing debate about the best way forward. The following questions are designed to generate further discussion about practical solutions to this complex issue.

- What are the major ways in which censorship can be treated as a trade issue? What are the advantages and disadvantages to going through the WTO to address Internet freedom issues? What other bodies and trade organizations might be effective on a global scale?

- What are the ways in which the economic impacts of restricted information flow over the Internet can be quantified, and how might these types of data be used to advance Internet freedom globally?

- How can companies, governments and civil society best address the issue of intermediary liability? How should they respond to competing pressures from users, national governments, local laws, and international norms?

- Is it feasible to rely solely on individual, self-generated corporate codes of conduct to protect Internet freedom, as many technology companies would prefer? Or would self-generated codes without third-party assessment prove ineffective and a continuation of the status quo, as many civil liberties and human rights NGOs argue? If self-generated codes of conduct are employed, how can they be made effective without independent oversight, and how can they represent progress from the current situation? Is there a hybrid model?

- What are the models that might apply to a codified approach toward enhancing Internet freedom? Some have suggested looking at the Foreign Corrupt Practices Act (FCPA), which subjects companies to possible penalties if they do not have corruption-prevention systems in place, as one model. What might be the benefits and drawbacks of this model or others?

- What are the pros and cons of national and/or intergovernmental regulation/legislation to protect freedom of expression and privacy on the Internet? What are the benchmarks that can help determine when a regulatory response is appropriate and when it overreaches?

- Some have argued that the Internet should be subject to an international governance regime similar to those governing other global commons. What might be the pros and cons of such a regime?

- To date, technology companies have essentially addressed government censorship and monitoring demands on a case-by-case basis, leaving individual companies to face complex Internet freedom issues on their own. What are the advantages and drawbacks to this piecemeal approach? What might a global, multistakeholder approach to Internet freedom look like?

- Looking ahead, the cloud computing environment, with its emphasis on central computer data storage rather than end-user terminals, raises additional concerns about government censorship and privacy issues, particularly if servers hosting cloud applications are hosted in authoritarian regimes. What types of policy frameworks will address data privacy and security in the cloud? How might local restrictions on the flow of information affect cloud computing?