Current Threats to Internet Freedom
Testimony to the Tom Lantos Human Rights Commission
Daniel Calingaert, Deputy Director of Programs, Freedom House
June 18, 2009

Chairman McGovern, Chairman Wolf, Honorable Members, thank you for the opportunity to speak to you today about the growing threats to Internet freedom in the world. These threats undermine the free flow of information, which is the lifeblood of a democratic society.

The Internet and other digital media have expanded space for citizens to express their views freely, but in response, repressive regimes have employed increasingly diverse and sophisticated controls on the Internet. These regimes have strengthened their ability to censor online content, to monitor Internet users, and to collect personal data, which they use to intimidate and prosecute their critics.

The rights of Internet users are increasingly at risk due to sophisticated methods of repression, such as targeted restrictions on social networking applications, manipulation of online discussions to drown out government critics, and "outsourcing of censorship," whereby governments require private companies—Internet service providers, blog hosting companies, cybercafés, and mobile phone operators—to monitor and censor users. Moreover, there still are cases where European and U.S. companies appear complicit in efforts by repressive regimes to filter online content and to spy on human rights advocates.

The greatest threats to Internet freedom are evident in China and Iran, where pervasive, multi-layered systems of censorship and surveillance stifle free expression on the Internet. These systems place severe limits on politically sensitive content that citizens can access, post on the Internet, and transmit via mobile phones. Surveillance of Internet and mobile phone communications is pervasive, and citizens who criticize the government online are subject to harassment, imprisonment, and torture.

In less restrictive settings, for instance in Egypt, Malaysia, and Russia, the Internet has emerged as a haven of relatively free speech in otherwise restrictive media environments. The space for free speech, however, is slowly closing, as governments devise subtle methods to manipulate online discussion and apply deliberately vague security laws to intimidate and arrest bloggers. This intimidation leads to self-censorship among journalists and commentators.

In just the past few weeks, we have seen stark reminders of the growing threat to Internet freedom. Following the June 12 presidential election in Iran, the government intensified its Internet filtering, disrupted social networking sites such as Facebook, and jammed transmissions of text messages on mobile phones in an apparent attempt to prevent Iranian citizens from voicing their suspicions of electoral fraud.

China's government has required that new "Green Dam" filtering software will be pre-installed on all personal computers sold in the country as of July 1. This software, ostensibly intended to block "unhealthy and vulgar" material, is in fact a Trojan horse that filters politically sensitive content, facilitates invasions of online privacy, and has the capacity to suddenly close applications like Microsoft Word when certain blacklisted terms are detected. The Green Dam software censors such politically sensitive content as the 1989 crackdown on pro-democracy protesters in Tiananmen Square and even blocks pictures of the cartoon character Garfield. This software also allows authorities to easily infiltrate a user's computer to monitor his or her Internet activity and to steal personal data.

Assessment of Internet Freedom

To improve understanding of the threats to free expression online, Freedom House released a report on April 1, 2009 entitled *Freedom on the Net: A Global Assessment of Internet and Digital Media* (available at http://www.freedomhouse.org/template.cfm?page=383&report=79&group=19). This report presents a new methodology to analyze and track Internet freedom globally and applies this methodology in 15 country reports, which assess Internet freedom in different regions of the world and span the range of experiences from free to highly repressive environments for Internet freedom. Funding for this report was provided by the U.S. Department of State, U.S. Agency for International Development, and Dutch Ministry of Foreign Affairs.

In its assessment of Internet freedom, Freedom House applies the same standard to all countries, irrespective of geographic location, ethnic or religious composition, or level of economic development. This standard is derived in large measure from Article 19 of the Universal Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."

The *Freedom on the Net* methodology measures Internet and digital media freedom on the basis of access to relevant information and communications technologies, including mobile phones and text messaging services, and of the free flow of information online. The methodology is particularly concerned with the exchange of news and other politically relevant content, the protection of users' rights, and the ability of citizens to use information and communications technologies for activism. It is organized into three categories of analysis:

1. *Obstacles to access*, including control over Internet service and mobile phone providers, Internet infrastructure, and economic barriers to access
2. *Controls on content*, such as legal regulations, blocking of websites, self-censorship, and the vibrancy of online news media
3. *Violations of users' rights*, including surveillance, infringements on privacy, and repercussions for online activity, such as fines or imprisonment

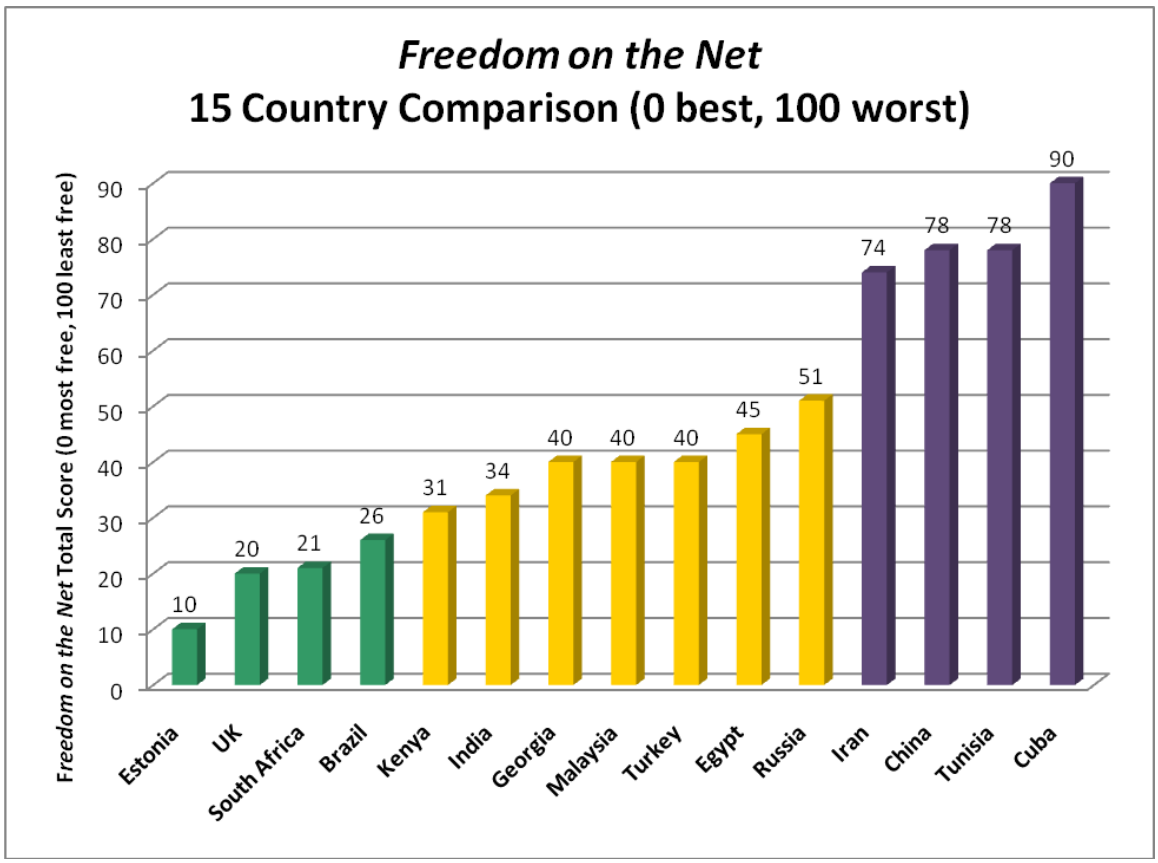
Across these three categories, there are a total of 19 questions to assess various aspects of Internet freedom. Countries are given a score for each of the three categories and a total score from 0 (best) to 100 (worst). A score of 0 to 30 represents a "Free" Internet and digital media environment; 31 to 60 is "Partly Free"; and 61 to 100 is "Not Free." A country report accompanies the scores and provides narrative detail on the methodology questions. The numerical scores serve to track trends in Internet freedom over time and allow for comparisons across countries.

Extent of Repression

The Internet and digital media environment varies widely by country, from highly restricted to very open. The worst of the 15 countries surveyed is Cuba, which received a score of 90 out of 100. Cuba stands out for its almost absolute control over the Internet. Access to the Internet and mobile phones is heavily restricted; the ability of citizens to use digital media as news sources or social networking is severely limited; there is hardly any regard for privacy rights; and critics of the regime face stringent legal penalties and intense harassment.

While Cuba maintains near-total restrictions on Internet access, other Not Free countries promote Internet use but control content and curtail free speech online. China, Iran, and Tunisia place significant restrictions on certain technologies and exercise extensive controls on content. They also resort to systematic violations of user rights, through surveillance of online activity, collection of personal data, and prosecutions and extra-legal attacks on dissidents. China has developed the most sophisticated apparatus to censor and control content, while the infrastructure in Iran and Tunisia places greater limitations on usage. Although there is more space for free expression on the Internet than in traditional (broadcast and print) media, all three governments take a range of measures to control digital media, particularly when it is used to mobilize political opposition.

The Partly Free countries range from the relatively strong performers—India and Kenya—to the more restrictive—Egypt, Georgia, Malaysia, Russia, and Turkey. These countries have some limits on access, either due to poor infrastructure or imposed by the government. They exert some control or state influence over content and over the ability of citizens to mobilize online. User rights are violated to varying degrees and include legal repercussions for online expression, interference in privacy, and physical harassment or attacks. In many of the Partly Free countries, there is a wide gap between Internet freedom and freedom of traditional media, and digital media provide relatively open outlets in what are otherwise difficult environments for freedom of expression. The governments of Egypt, Malaysia, and Russia encourage expanded access to the Internet and impose relatively little censorship, but they monitor Internet activity quite extensively and impose harsh penalties on their online critics.



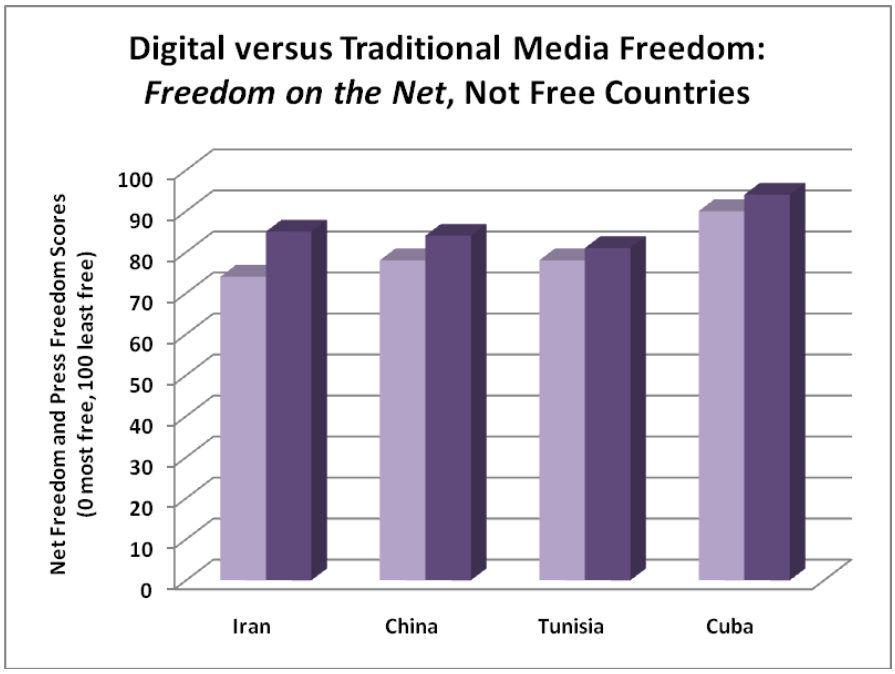
The threats to Internet freedom go far beyond the countries covered in *Freedom on the Net* study. For example, online journalists were arrested last year in several additional countries, such as Burundi, Uzbekistan, Burma, and Vietnam, and political content was filtered in countries across the Middle East (Libya, Saudi Arabia, Syria, and elsewhere), in former Soviet Union (Belarus, Azerbaijan, Uzbekistan), in south-east Asia (Burma, Thailand, and Vietnam), and into Africa, for instance in Ethiopia.

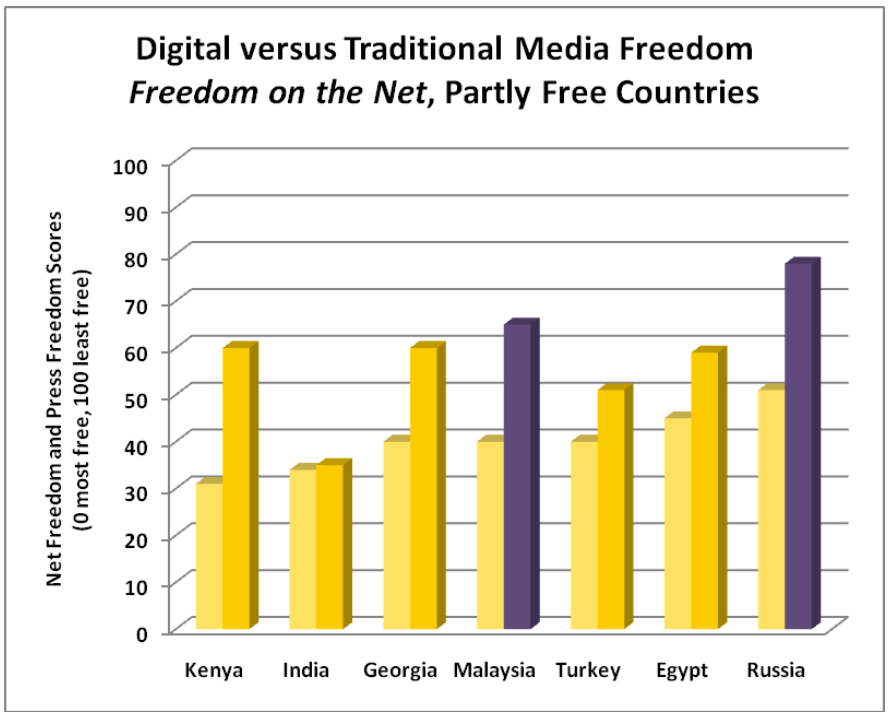
In Free countries, Internet freedom is thriving but cannot be taken for granted. Even in a bastion of democracy, such as the United Kingdom, Internet freedom suffers from harassment of online commentators due to libel laws, opaque procedures for filtering content, and extensive surveillance.

Digital Media's Potential

The mounting assault on Internet freedom is taking place against the backdrop of explosive growth in the use and the influence of digital media. The number of Internet users has increased exponentially; it has, for example, more than doubled in China and Egypt from 2006 to 2008. Recent years have also featured a "blogging revolution," as millions of citizens have begun to write online journals and share opinions on a vast range of cultural, social, and political issues. The number of bloggers in China has reportedly risen to 50 million, with a total of more than 100 million blogs. The bounds of free expression usually are pushed by bloggers, in China and elsewhere.

The Internet and other digital media have provided avenues to circumvent restrictions on broadcast and print media and increased opportunities to enrich public discourse, expose abuses of power, and facilitate citizen activism. All of the 15 countries surveyed—with the exception of the United Kingdom—received a higher score for Internet freedom than for overall media freedom, as measured on the same 0 to 100 scale by Freedom House's *Freedom of the Press* survey. The difference in scores for Internet freedom and traditional media freedom was most pronounced among Partly Free countries.





Citizens are finding inventive ways to create and spread information. They are gaining access to censored content through circumvention technologies and avoiding government blocks on their blog posts by using code or images for sensitive keywords that trigger filters. Citizens are adding to the diversity of opinions online, drawing attention to abuses of power, and organizing protests through social networks like Facebook.

The response to the introduction of Green Dam censorship software in China provides just the most recent example of citizens using the Internet to stand up to repressive regimes. Numerous experts in China tested the software, and word about its harmful effects spread rapidly online. Ordinary citizens voiced strong objections to the software and used social networking tools to organize online protests against the Green Dam.

The horizontal nature of the Internet, whereby ordinary users can easily generate content and share information among social networks, empowers citizens in ways that traditional broadcast and print media cannot. Tens of millions of citizens in repressive environments have, through the Internet, become commentators and media producers and built their own audiences. As a result, free expression is far more difficult to control in digital media than in traditional media. At the same time, however, controls on digital media are more intrusive and directly affect much larger numbers of citizens. Internet censorship, for example, infringes on the rights of a great many citizens as content producers, not only as consumers, and online surveillance allows authorities to monitor personal communications as well as to track what citizens read.

Methods of Control

A variety of methods are used, often in combination, to curtail Internet freedom. These methods include the following:

- *Expanding forms of censorship*: The OpenNet Initiative has documented a dramatic increase in the practice of filtering over the past several years, with a growing number of countries engaging in this practice. Technical filtering can affect either specific content or broad swaths of information at the Internet service provider (ISP) level. It can target keywords, particular web addresses, or entire domain names. Moreover, repressive regimes use a range of additional methods to control the circulation of information online. They employ human censors to monitor and manually remove blog postings; outsource search-engine filtering and chat-room censorship to private companies; and resort to judicial orders, regulator instructions, or informal requests to ISPs, websites, or blog hosts to take down proscribed material. China, Iran, and Tunisia use systematic technical means to filter political content. They are able to do so because they have centralized their Internet infrastructure so that all traffic must pass through a limited number of gateways or service providers, particularly to connect to the global Internet. In these countries, there is pervasive filtering of taboo subjects, such as human rights violations, prominent political figures, oppressed minorities, and official corruption. Proscribed content is identified through lists of forbidden keywords or website addresses, and these lists are regularly updated by state

agencies. Other countries eschew extensive filtering but still impose serious blocks on specific websites or types of political content, such as opposition news sources in Malaysia. Russian authorities rely to a larger extent on behind-the-scenes pressure or phone calls to demand removal of certain content.

- *Restricted access to technologies or applications*: Seven of the 15 countries surveyed—Brazil, China, Cuba, Georgia, Iran, Tunisia, and Turkey—had blocked Web 2.0 applications temporarily or permanently during the period covered in the study, calendar years 2007 and 2008. These applications include the social-networking site Facebook, the video-sharing site YouTube, and the blog-hosting site Blogspot. The restrictions imposed by China and Tunisia were limited in scope. They sporadically interfered with access to Web 2.0 applications around particular events or selectively targeted specific activists. Iran, however, denies access to broadband to the majority of its Internet users.

- *"Outsourcing" of censorship*: Rather than rely entirely on direct intervention by government agencies, repressive regimes increasingly "outsource" censorship and surveillance to private companies—to Internet service providers, blog-hosting companies, cybercafés, and mobile phone operators. In repressive environments, such as China, Cuba, Egypt, Iran, and Tunisia, outsourcing involves extensive surveillance and user registration, particularly in cybercafés. There are legal requirements for private companies to filter political content, monitor Internet activity, and collect data on Internet users. Companies that fail to comply with these requirements risk fines or loss of their business license. In China, surveillance of Internet and mobile phone communications is pervasive. Users are required to register with an ISP when they purchase Internet access at home or at work, so that authorities can track their online activity. Customers at cybercafés have to present identification, and cybercafés must install software to monitor and filter customers' web browsing.

- *Lack of transparency*: Few of the countries surveyed provide significant transparency regarding censorship decisions or surveillance. They provide no public list of blocked websites and offer little possibility to appeal decisions on filtered content. Moreover, when authoritarian regimes use information that is obtained from monitoring the content or the traffic data of Internet or mobile-phone communications, there is no independent judicial supervision.

- *Content manipulation*: Repressive regimes increasingly resort to the clandestine use of paid pro-government commentators or financed websites or blogs to influence or guide online discussions. The Chinese government employs an estimated 250,000 or more "50 Cent Party" commentators, while Russia has seen a proliferation of Kremlin-affiliated "web brigades," and Tunisia uses a smaller team of undercover agents, all to subvert any online conversations that might erode support for the regime. A related dynamic is the spillover effect of tightly controlled traditional media outlets that launch online versions, remain key

sources of information for many ordinary citizens, and are thus able to shape online opinions.

- *Legal repercussions*: Authoritarian governments use general press laws or statutes against insult, blasphemy, leaks of state secrets, etc., to punish online dissidents. In 8 of the 15 countries surveyed—China, Cuba, Egypt, India, Iran, Malaysia, Russia, and Tunisia—a blogger or online journalist was arrested during the coverage period. Cuba is one of the few countries with Internet-specific legislation but tends to prosecute online journalists under generic charges such as presenting a "pre-criminal social danger." China has the highest level of prosecutions. It uses laws against "inciting subversion," "leaking state secrets," and "using a heretical organization to undermine the law," and has issued more than 80 decrees that specifically address Internet content and related issues. Prison sentences for online violations in China typically range from three to ten years, while in other countries, most sentences range from six months to four years. Numerous prosecutions have also occurred in Tunisia, Iran, Egypt, and Malaysia, where laws against insulting the head of state or Islam are most frequently invoked, while Russia relies on vague laws against extremism. In the United Kingdom, the phenomenon of "libel tourism" has led to self-censorship among both traditional and online commentators. Wealthy individuals from the Middle East and the former Soviet Union have exploited expansive interpretations of libel laws and jurisdictional questions by British courts to silence or intimidate journalists through civil lawsuits.

- *Extralegal harassment and threats*: According to the Committee to Protect Journalists, there were more online journalists than traditional journalists behind bars for the first time in 2008, as a result of either legal prosecution or extralegal detention. Intimidation of bloggers and online journalists has reached significant proportions in China, Egypt, Iran, and Tunisia, where multiple individuals have been subjected to arbitrary arrest, 24-hour surveillance, harassment, prosecution, or various forms of mental and physical mistreatment, including torture. Egypt stands out as a country with a relatively open Internet environment that resorts to harassment to make an example of a few prominent activists and bloggers. Although the number of individuals targeted in these countries in small, compared to the entire online community, their experiences have a chilling effect on their peers.

- *Technical attacks*: A particular form of harassment against bloggers and online activists is "technical violence." Blogs and websites are hacked or subjected to denial-of-service attacks, which disrupt or shut down the sites. In Estonia and Georgia, massive denial-of-service attacks targeted government websites and information networks during periods of diplomatic tension or military conflict with Russia. These attacks were apparently carried out by individuals who were resident in Russia and possibly associated with Russian authorities.

Involvement of Western Companies

Technology from European and U.S. companies continues to contribute to the efforts by repressive regimes to restrict freedom of digital media. In April, news reports revealed that Nokia Siemens Networks delivered a monitoring center to IranTelecom, Iran's state-owned telephone company. This center allows authorities to tap mobile phones and monitor electronic data transmissions. Nokia Siemens Networks is a joint venture of the Finnish cell-phone giant Nokia and the German electronics and electrical engineering company Siemens, which has, since 2005, done more than $900 million worth of business with the U.S. government.

Human rights advocates and intelligence experts believe that IranTelecom's new monitoring center provides an electronic surveillance system to target dissidents. This surveillance system probably has enhanced the capacity of Iranian authorities to monitor private communications. According to the International Campaign for Human Rights in Iran, for example, government interception of private communications led to the arrest of 12 women's rights activists in March.

In a separate case, reported last month, a city library in Mississauga, Canada was found to use web-filtering technology similar to that used in China. This technology blocked websites that addressed topics the Chinese government considers sensitive, such as controversies surrounding the 2008 Olympics, repression of Tibetans, Falun Gong, and repression of Christians in China. The library in Mississauga, Canada lacked the manpower to review all of the blocked websites, particularly the websites in Mandarin, and thus relied on the software company to decide which websites to block.

The filtering software was developed by SurfControl and sold to the Mississauga library by Websense, which had acquired SurfControl in 2007. This SurfControl software is used by a variety of libraries in different countries. The China-specific filtering settings apparently were the default settings in the version of the software sent to the Mississauga library. The sale of this software by Websense suggests that Chinese standards for filtering are making their way into other countries, even without the knowledge or consent of the software purchasers.

Supporting Internet Freedom

U.S. policy to protect Internet freedom should, at a minimum, ensure that U.S. companies are no longer complicit in violations of Internet users' rights. The Global Online Freedom Act (GOFA) is critical to promote freedom of expression and expand the flow of information on the Internet. GOFA would require U.S. companies to host personal data outside of the reach of Internet-restricting governments; give the Attorney General the authority to deny requests for personal data that might be used to repress dissidents; prevent U.S. companies from blocking access to U.S. government-supported websites; and require U.S. companies to disclose the methods of filtering they use and the content they block at the request of repressive regimes. In addition, GOFA would create an Office of Global Internet Freedom in the State Department and explore the feasibility of

introducing export controls on filtering and surveillance technologies to Internet-restricting countries.

While voluntary codes of conduct, such as the Global Network Initiative, are commendable, they are insufficient to shield U.S. companies from pressure to filter content or to turn over personal data on peaceful dissidents. GOFA will provide strong protection to U.S. companies against such pressure.

Rather than put U.S. companies at a competitive disadvantage, GOFA is likely to raise international standards for business to protect and advance Internet freedom, much as the Foreign Corrupt Practices Act led to the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

But GOFA is not enough. Further policy initiatives are needed to defend and expand Internet freedom:

1. The State Department should engage in more rigorous diplomacy in support of U.S. companies as they seek to avoid pressure to limit access to content or weaken protections on the personal data of Internet users. This diplomacy should both challenge violations of Internet freedom by repressive governments and build broader coalitions among democratic governments to advance Internet freedom. The State Department should also seek to persuade democratic governments to adopt similar controls as the United States on exports of Internet censorship and surveillance technologies to Internet-restricting countries.

2. The U.S. Trade Representative should explore the possibility of resisting Internet censorship within the context of bilateral and multilateral negotiations or of challenges to trade barriers before the World Trade Organization.

3. Congress should expand its efforts to advance Internet freedom, for instance to draw attention to human rights abuses against Internet users, as Congressmen Barney Frank, Trent Franks, and Mark Kirk have done in the case of arrested Egyptian blogger Kareem Amer. These efforts should draw attention both to individual cases of human rights abuse and to broader violations of Internet freedom, such as the sophisticated, multi-layered systems of Internet censorship used in a growing number of countries.

4. The U.S. government and other democratic governments have funded important Internet freedom programs. Greater support is needed to advance indigenous efforts within Internet-restricting countries to expand the space for free expression online. A multi-donor fund would bolster the shared commitments of democratic governments to provide such support. Such a fund is needed to:

    - expand education and exchanges with experts (academics, journalists, lawyers, etc.) in repressive environments on issues of online censorship and privacy

- enhance advocacy by the experts on Internet freedom
- provide direct support to victims of repression, such as arrested bloggers
- build networks of Internet freedom advocates across Internet-restricting countries, so that they may learn from each other's creativity in challenging repression
- facilitate translations of material related to freedom of expression online
- increase research on Internet censorship and violations of user rights
- stimulate development of and expand access to innovative technologies to circumvent censorship and to protect personal data

Through the adoption of the Global Online Freedom Act, rigorous diplomacy, support for free speech advocates in repressive environments, and Congressional engagement, the United States can lead international efforts to protect and advance freedom of expression online. At a time when the rights of Internet users across the globe are increasingly at risk, U.S. leadership is critical to defend Internet freedom, so that citizens living under authoritarian regimes may still find a space to speak openly, to connect with like-minded citizens, and to hold government to account.