Law&Ethics

The Global Online Freedom Act

Ian Brown

The wide diffusion of the Internet in developed and developing nations has made it a key medium for political debate and activism. Social media tools like Facebook, Twitter, YouTube, WordPress, and other platforms can give individuals and small campaign groups a reach that was previously only available to much larger organizations.[1] These sites were all used by campaigners for regime change in Egypt, Libya, Yemen, and Tunisia during the "Arab Spring." They continue to play a role in events in Syria, Bahrain, and Iran. As German Foreign Minister Guido Westerwelle told a Berlin conference in September 2012, "The Internet offers new opportunities for advocates of freedom in authoritarian regimes to communicate with one another. It allows the online documentation of human rights violations that previously could be covered up. And it gives bloggers and activists the chance to raise their voice in societies where traditional media can be easily controlled."[2]

However, some repressive governments have developed sophisticated systems for monitoring and profiling online communications and activism, with extremely serious consequences for their political opponents, from harassment and arrest up to torture and death. Many of these systems

Dr. Ian Brown is associate director of Oxford University's Cyber Security Centre, where he has led several major research projects for the European Commission, OECD, and UK government. He has consulted for the U.S. Department of Homeland Security and a number of other public and private sector organizations. His next two books, both being published in March 2013, are *Regulating Code* (MIT Press) and *Research Handbook on Governance of the Internet* (Edward Elgar).

are based on technology exported from democratic states with constitutional commitments to human rights.[3] In its 2012 annual report, Freedom House found that 19 out of 47 countries surveyed had passed new laws since January 2011 restricting online speech, violating user privacy, or punishing individuals for objectionable or undesirable posts.[4]

Recognizing the Internet's potential as a tool for freedom of expression and democratization, a number of governments have taken steps to reduce the flow of surveillance technologies to repressive regimes, while promoting training and the development of free speech tools for activists. U.S. Secretary of State Hillary Clinton has made several speeches on "Internet freedom," identifying online freedom of expression as a foreign policy priority and committing tens of millions of dollars to measures aimed at the regimes of China, Syria, Cuba, Vietnam, and Myanmar.[5] At the intergovernmental level, the UN Human Rights Council has affirmed that human rights are equally protected in the online environment under the International Covenant on Civil and Political Rights.[6]

Many of these systems are based on technology exported from democratic states with constitutional commitments to human rights.

In the United States, the Global Online Freedom Act (GOFA) of 2011 (H.R. 3605) would complement the Obama administration's efforts to promote Internet freedom. Sponsored by New Jersey Representative Christopher Smith, the bill would require the Secretary of State to designate "Internet-restricting countries" each year and to include an assessment of "freedom of electronic information" in annual country reports on human rights practices. Internet companies listed on U.S. stock exchanges and operating in designated countries would be required to publish in their annual reports policies addressing human rights due diligence, disclosure of personally identifiable information to such governments, and transparency of restrictions on search engines and content hosting services. This would affect a broad range of international companies, including, for example, China Mobile and Baidu. Controls would be imposed on the export of goods and technology serving the primary purpose of assisting foreign governments in carrying out Internet censorship or surveillance. The bill was reported favorably out of committee on 27 March 2012 and, according to its sponsors, is likely to be reintroduced in 2013.

This article analyzes in more detail the provisions of GOFA, looking at the problems addressed by the bill, and making suggestions as to where additional action may be required to meet its objectives.

Background. A number of democratic governments have made the pro-

motion of online freedoms an explicit goal of foreign policy. The G8 2011 declaration included a commitment "to encourage the use of the Internet as a tool to advance human rights and democratic participation throughout the world."[7] European states such as the UK, Germany, Sweden, the Netherlands, and France have made ministerial statements and organized conferences addressing this commitment, such as the September 2012 German Foreign Ministry event in Berlin on "The Internet and Human Rights: Building a free, open and secure Internet." Intergovernmental organizations such as the Organization for Security and Cooperation in Europe and the Council of Europe have published reports and instituted programs of work on the protection of online rights.[8]

In the United States, the Global Online Freedom Act (GOFA) was first introduced in Congress in 2006 as H.R. 4780, after Chinese dissidents Shi Tao and Li Zhi were imprisoned following the disclosure of account information by Yahoo! to the Chinese authorities. The sponsor, Representative Christopher Smith, remarked that "for the sake of market share and profits, leading U.S. companies like Google, Yahoo!, Cisco, and Microsoft have compromised both the integrity of their product and their duties as responsible corporate citizens. They have aided and abetted the Chinese regime to prop up both of these pillars, propagating the message of the dictatorship unabated and supporting the secret police in a myriad of ways, including surveillance and invasion of privacy, in order to effectuate the massive crackdown on its citizens."[9]

Further versions of the bill were introduced in 2007 (H.R. 275), 2009 (H.R. 2271), and April 2011 (H.R. 1389). The current version of the bill (H.R. 3605) was introduced in December 2011 and approved by the House Committee on Foreign Affairs' Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations on 27 March 2012. This version has corporate support (from Yahoo!) as well as support from human rights groups.

Provisions of the Act. GOFA section 101 defines freedom of opinion and expression as "a fundamental component of United States foreign policy" that should be promoted using "all appropriate instruments of United States influence." It requests that the president seek the agreement of other nations to promote the goals of the Act, and encourages U.S. businesses to limit censorship and ensure access to websites such as Voice of America and the State Department's reports on human rights practices, international religious freedom, and human trafficking (sec. 102).

The Act then makes provisions in three main areas: human rights reporting, corporate transparency, and export controls on telecommunications equipment.

Human Rights Reporting. GOFA section 103 would amend the Foreign Assistance Act of 1961 to require "an assessment of the freedom of expression with respect to electronic information" in annual reports on countries receiving economic and security assistance. Some of this information is already included in the State

Department's country reports on human rights. Section 105 instructs the U.S. Trade Representative to report to Congress on trade disputes arising from government censorship and efforts to resolve these disputes.

Each year, the Act would require the Secretary of State (after consulting the Secretary of Commerce) to designate "Internet-restricting countries" whose governments are "directly or indirectly responsible for a systematic pattern of substantial restrictions on Internet freedom" (sec. 104). Likely candidate countries were explicitly named in the 2007 version of the bill: Belarus, Cuba, Ethiopia, Iran, Laos, North Korea, the People's Republic of China, Tunisia, and Vietnam. This provision is similar to special watch list mechanisms in legislation concerning human trafficking and state sponsorship of terrorism.[10]

Corporate Transparency. Internet infrastructure and services are operated largely by the private sector, so corporate social responsibility is critical for the protection of online freedoms. Transparency about company policies impacting on Internet freedom allows individuals to choose service providers that act in accordance with their own values, and socially responsible investors to avoid providing capital to firms that are contributing to human rights violations.

GOFA section 201 requires U.S.-listed Internet Communications Services companies operating in Internet-restricting countries to include in their annual reports information on company policies on human rights due diligence, based around the OECD's Guidelines for Multinational Enterprises. Companies that collect personally identifiable information or communications are required to include a summary of policies on how they will respond to requests by governments of Internet-restricting countries for disclosure of this information. Section 201 also requires that search engines and content hosting companies include information on the steps they take to give users notice when an Internet-restricting country has requested that specific information be blocked. A safe harbor is provided from these requirements for companies that are a member of the Global Network Initiative or other multi-stakeholder initiative that includes civil society organizations, promotes the rule of law, allows for the freedom of expression and privacy, and requires independent assessments of compliance.

Section 201 is modeled on sections of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, related to the extractive industries, and on conflict minerals and mining in the Democratic Republic of Congo and its neighbors.[11] Those parts of the Dodd-Frank Act were opposed by industry groups, such as the U.S. Chamber of Commerce, but supported by some computing companies, including Hewlett-Packard, AMD, Motorola, and Microsoft.

This section should improve Internet industry transparency, which is important given that some companies have previously refused to provide this information even after their products were discovered in government buildings following the overthrow of repressive regimes in countries such as Libya.[12]

Export Controls. Sanctions against Syria and Iran imposed by the United States and EU already include restrictions on technology exports that could be used in human rights violations. The United States added further controls in 2011 on companies that "create or operate systems used to monitor, track, and target citizens for killing, torture, or other grave abuses."[13]

However, sanctions are difficult for states to agree on, sometimes easy to circumvent, and limited to a small number of targets. They often come too late to prevent surveillance capabilities being built into networks that may later be used for repression after a change in government policies and personnel, or in situations that have not yet deteriorated into a condition of non-international armed conflict.[14]

Human rights groups have therefore campaigned for surveillance and censorship technologies to be added to broader export control regimes. GOFA section 301 would amend the Export Administration Act of 1979 to add a category of controlled goods and technology whose primary purpose is to assist foreign governments in Internet censorship and surveillance. Exports of such goods to Internet-restricting governments would be prohibited, except where the president issues a waiver "in the national interests" of the United States.

Analysis. The majority of the provisions of GOFA relate to transparency, through the annual publication by the State Department of information about Internet freedom in states receiving economic and security assistance, and the disclosure of corporate policies related to Internet blocking and surveillance by U.S.-listed Internet Communications Services companies. These parts of the Act are relatively uncontroversial, although civil society experts and groups such as Access have warned that the process of designating Internet-restricting countries could become politicized, with factors unrelated to human rights determining the designation or otherwise of countries such as U.S. ally Bahrain.[15] Designation of a government would support some level of public approbation and diplomatic pressure. Disclosure of inadequate corporate policies by companies would enable divestment by socially responsible investors, raising (by a small amount) their cost of capital, and provide evidence that could be used by civil society in public campaigns. It may, however, lead to the sale of company divisions responsible for affected products, as happened for instance with former Nokia Siemens subsidiary Trovicor following criticism for its sales of telecommunications monitoring technology to Iran.[16]

Civil society groups suggest that Internet companies and human rights organizations have a stronger input into the designation process – as GOFA already envisages in the assessment of electronic freedom in foreign countries. In addition, the Electronic Frontier Foundation suggests the publication of all evidence related to the assessment of countries not designed as Internet-restricting, and that transparency requirements are extended from Internet communications services to technology companies and providers of other services that might be used for surveillance and censorship.[17] Broad-

ening reporting requirements to a wider range of countries would improve the information available on countries such as India and Thailand that are censoring the Internet without reaching the level that would justify full designation as Internet-restricting.[18]

Export controls are much more controversial, which is why GOFA's provisions are narrowly drawn. It can be difficult to specify precisely potentially repressive technologies. Equipment that can be used to monitor and block Internet communications is widely available, and has a number of legitimate uses. "Deep Packet Inspection" equipment is used by ISPs for network management and security and for building advertising profiles of users, as well as for communications surveillance. Firewalls can block "denial of service" attack traffic and malicious software.

Almost every state imposes "lawful interception" requirements on communications companies, requiring they be able to give police and intelligence agencies access to voice and data communications subject to administrative or judicial warrant. High capacity links inside large ISP networks can require expensive equipment to fully monitor, but many authoritarian states are mainly interested in surveillance of their own low-bandwidth international network links. Real-time blocking and surveillance capabilities are not necessary for repressive states, only the means to identify users accessing politically sensitive websites for later questioning.

Many states with weaker freedom of speech protections than the U.S. require ISPs to block access to sites featuring illegal material such as child abuse images, material inciting religious and racial hatred, and certain types of banned services such as online gambling. It is extremely difficult to ensure surveillance and blocking tools are only used for these legitimate purposes, with appropriate levels of transparency and accountability.

Export controls must be carefully targeted to avoid rules that can easily be bypassed by the production of controlled items outside the control regime. Communications equipment is usually portable, and is less familiar to customs officials than weapons and other equipment covered by controls. Software is especially difficult to control, given how easily it can be transferred across borders via the Internet. A well-known example is the use in Syrian telecommunications networks of web filtering and blocking devices from U.S. company Blue Coat, which were illegally transferred to Syria by a distributor in the United Arab Emirates.[19] Controls are only likely to be effective against products and services that require significant expertise and investment to reproduce outside the U.S. (and its partners in international control regimes, such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies).

Another serious problem is that technologies useful to human rights activists can be blocked by sanctions and broader export controls. Syrian activist Delshad Othman told *The Washington Post* in August 2012 that sanctions had made it much harder for activists to use anti-tracking software, meaning that "they are filming and uploading pictures without protection, so the regime can easily arrest them or even kill them." Even though

the Obama administration has created exemptions to allow the export of these kinds of tools, the complexity of controls and licensing procedures, and harsh penalties for making a mistake, still discourage firms from risking exports that should be allowed.[20] The Electronic Frontier Foundation has praised the limiting of GOFA's export controls to government end users and suggested there should be an easy process to challenge any controls imposed.[21]

There is potential for refining the type of export controls contained in GOFA. Telecommunications companies are often closely linked to governments, and heavily regulated in most countries, but would remain free to import high-performance surveillance and blocking equipment under the bill.

Such systems are now frequently updated and patched remotely by their vendors. Some use hard to bypass "Digital Rights Management" functionality to enforce restrictions such as the number of simultaneous users. They often require post-installation configuration and staff training by their vendor. These channels all provide further opportunities to restrict the use of such systems for serious violations of human rights.

Careful diplomacy will be needed with other states if a workable international framework is to be established. Russia's Foreign Ministry has reportedly criticized GOFA, stating: "It seems as if some members of the American establishment are taking a confrontational mentality and surviving schemes of the Cold War to web technologies."

Russia and a number of other states would prefer a treaty negotiated within the UN.[22] However, the International Code of Conduct for Information Security proposed to the UN General Assembly by China, Russia, Tajikistan, and Uzbekistan has itself been strongly criticized for its impact on human rights.[23] In the medium term, the U.S. is more likely to make progress towards protecting Internet freedom by working with traditional allies such as Canada and EU Member States. These countries are promoting the development of norms for responsible online behavior rather than a treaty-based approach.

Conclusion. The Global Online Freedom Act is one of the most comprehensive legislative attempts to protect online human rights. If passed, it would improve the understanding of foreign government attempts to censor and persecute political opponents by requiring the State Department to publish annual reports on Internet accessibility, surveillance, and freedom of expression in countries receiving economic and security assistance. It would require transparency on human rights due diligence and policies from U.S.-listed companies providing Internet communications services in designated "Internet-restricting" countries, particularly search engines and content hosts. More controversially, it would impose controls on the export to Internet-restricting governments of goods and technology that have the primary purpose of assisting censorship or surveillance. Civil society groups have concerns that such controls could block the availability of tools useful for human rights activists in affected countries.

More broadly, governments need to provide more incentives for multinational companies to comply with the UN Guiding Principles on Business

and Human Rights, which states, "the responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate."[24] Participation in multi-stakeholder groups such as the Global Network Initiative, co-founded by Google, Yahoo!, and Microsoft, is one obvious way for Internet companies to meet this standard.

For those that do not, and whose products are used by repressive governments in serious human rights violations, some form of civil liability may be appropriate. Two cases, *Du v. Cisco* and *Doe v. Cisco*, are attempting to establish this under the U.S. Alien Tort Statute and Torture Victim Protection Act.[25] However, the scope of the Alien Tort Statute may be restricted by a case before the Supreme Court, *Kiobel v. Royal Dutch Petroleum*.[26]

NOTES

Acknowledgments: *The author thanks David Sullivan and Jillian York for their helpful comments on a draft of this article.*

1 Rebecca MacKinnon, *Consent of the Networked* (New York: Basic Books, 2011).

2 Guido Westerwelle, "Rede Außenminister Guido Westerwelles anlässlich der Konferenz 'The Internet and Human Rights: Building a free, open and secure Internet'" (Berlin, 14 September 2012).

3 Evgeny Morozov, *The Net Delusion: How Not to Liberate the World* (London: Allen Lane, 2011).

4 Freedom House, *Freedom on the Net 2012 - A Global Assessment of Internet and Digital Media* (Washington, D.C., 2012).

5 Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World" (George Washington University, 15 February 2011).

6 UN Human Rights Council, "The Promotion, Protection and Enjoyment of Human Rights on the Internet" (Doc. A/HRC/20/L.13, 5 July 2012).

7 Group of 8, G8 Declaration: *Renewed Commitment for Freedom and Democracy* (Deauville, 27 May 2011).

8 Y. Akdeniz, *Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States* (Vienna: Organization for Security and Co-operation in Europe, 2010). Council of Europe, *Internet Governance 2012-2015: Draft Council of Europe Strategy* (Strasbourg, 2011).

9 Christopher H. Smith, "The Internet in China" (Congressional Record – Extensions of Remarks, E206, 28 February 2006).

10 David P. Fidler, "The Internet, Human Rights, and U.S. Foreign Policy: The Global Online Freedom Act of 2012," *American Society of International Law Insights* 16, no. 18 (24 May 2012).

11 *Ibid.*

12 Cindy Cohn, Jillian C. York and Trevor Timm, "Global Online Freedom Act 2012 Is An Important Step Forward," Internet, https://www.eff.org/deeplinks/2012/04/global-online-freedom-act (date accessed: 26 October 2012).

13 The White House, *Fact Sheet: A Comprehensive Strategy and New Tools to Prevent and Respond to Atrocities* (Washington, D.C., 23 April 2012).

14 Ian Brown and Douwe Korff, *Digital Freedoms in International Law* (Washington, D.C.: Global Network Initiative, 4 June 2012).

15 Access, "US bill to restrict sale of surveillance technology - a step in the right direction," Internet, https://www.accessnow.org/blog/us-bill-to-restrict-sale-of-surveillance-technology-a-step-in-the-right-dir (date accessed: 26 October 2012).

16 Trevor Timm, "Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA", Internet, https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa (date accessed: 26 October 2012).

17 See note 12.

18 Testimony of Rebecca MacKinnon to the House Foreign Affairs Subcommittee on Africa, Global Health, and Human Rights, 8 December 2011.

19 Blue Coat, "Update on Blue Coat Devices in Syria," Internet, http://www.bluecoat.com/company/news/statement-syria (date accessed: 26 October 2012).

20 James Ball, "Sanctions aimed at Syria and Iran are hindering opposition, activists say," *Washington Post*, 14 August 2012.

21 See note 12.

22 "Russia slams US Global Online Freedom Act as 'Cold War scheme'," *Russia Today*, 19 December 2011.

23 Katitza Rodriguez, "Hey ITU Member States: No More Secrecy, Release the Treaty Proposals," Internet, https://www.eff.org/deeplinks/2012/05/hey-itu-member-states-no-more-secrecy-release-wcit-documents-0 (date accessed: 26 October 2012).

24 John Ruggie, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework" (UN Doc. A/HRC/17/31, 21 March 2011): 13.

25 Maryland District Court, filed 6 June 2011; California Northern District Court, filed 19 May 2011.

26 132 S.Ct. 472 (2011).