

Technology Law

E-Commerce

Freedom of Speech

Proposed Global Online Freedom Act Could Impact Supply Chains, Outsourcing Efforts and Foreign Operations of U.S. and Multinational Companies



Moore&VanAllen

Contributed by Todd C. Taylor, Moore & Van Allen PLLC

On December 8, 2011, Congressman Chris Smith of New Jersey introduced a new bill in the House of Representatives entitled “The Global Online Freedom Act of 2011” (“GOFA”).¹ According to Congressman Smith, GOFA is a response “to the growing use of the Internet as a tool of repression, and to changes in the technologies of repression.”²

Perhaps not surprisingly, the Bill received swift criticism from countries that might be viewed as potential targets of the proposed legislation. On December 19, 2011, Aleksandr Lukashевич, a spokesman for the Russian Ministry of Foreign Affairs, claimed:

representatives of the US establishment are trying to shift the confrontational mentality and the surviving algorithms of the Cold War era into the area of modern digital technologies. The USA is once again seeking to act as supreme arbiter and ‘decider of the world’s fate,’ this time trying to put in its service the power of network technologies as a catalyst for political, social, and economic processes in states and regions vital to it.³

The Bill and the resulting criticism raise several issues. Is there a need for GOFA? Is GOFA as far reaching as its sponsors (and critics) claim? What impact will GOFA have on multinational businesses with U.S. operations? Will the Bill actually pass?

Why GOFA?

There are numerous studies and reports that lend support to Representative’s Smith claims that many foreign governments are using the Internet “as a tool of repression”.

According to a recent study by the Center for Technology Innovation at Brookings, since 1995 there have been 606 unique incidents involving governmental actors blocking or disrupting internet and digital communications traffic.⁴ Particularly concerning is the trend line on these incidents. The Brookings report claimed that there were 155 disruption or blocking incidents between 1995 and 2006, while there were 453 disruption or blocking incidents in the five-year period between 2007 and 2011.⁵ Reported examples of disruption and blocking events have included the blocking of Facebook and Twitter in China,⁶ deliberate slowing of internet speeds in Iran,⁷ blocking of an environmental website in Russia⁸ and YouTube blocking in Turkey.⁹

Many governments do not confine themselves to simply blocking or limiting internet traffic - at least according to some reports. There have been claims that the Iranian government has arrested and beaten opposition figures following extensive

Originally published by Bloomberg Finance L.P. in the Vol. 5, No. 2 edition of the Bloomberg Law Reports—Technology Law. Reprinted with permission. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

monitoring of such figures' cell phones, email accounts and text messaging activities.¹⁰ Prominent Chinese activists have received jail sentences in connection with their email and website based criticism of Chinese governmental actions.¹¹ In Tunisia, prior to the recent "Arab Spring" revolution in that state, its former government reportedly monitored the email traffic of its citizens and, at times, would even alter the content of email communications while in transit.¹²

Many European and American companies have been accused of aiding the internet blocking and surveillance activities of repressive regimes. For instance, Telecomix, a multinational group of online activists, found evidence that Blue Coat Systems, Inc., an American corporation, provided web filtering technology to the Syrian government.¹³ While several European companies, including Ericsson AB, Creativity Software, Ltd. and AdaptiveMobile Security Ltd., have been accused of providing equipment that was accessible by Iranian law enforcement and state security agencies.¹⁴

GOFA's Reach

As written, GOFA has three primary requirements:

- New Reports and Designations from the State Department. New reporting obligations are imposed on the U.S. Secretary of State.
 - The U.S. Department of State would be required to include in its annual country reports information related to whether such country's government (a) filters, censors or blocks internet content, (b) has punished individuals or groups for expressing political, religious or ideological opinions via the internet, and (c) has sought to collect, obtain or disclose personally identifiable information of a person in connection with such person's expression of political, religious or ideological belief.¹⁵
 - The Secretary of State would be required to annually designate any Internet restricting countries.¹⁶
- New Public Filing Requirements for Certain Publicly Traded Companies. Any "**Internet communications services company**" with securities trading on a U.S. securities exchange and operating in an "Internet restricting country" would be required to include the following information in its publicly filed annual report:
 - Information relating to its internal company policies addressing human rights due diligence.
 - Whether such internal company policies (a) have been approved at "senior levels" of the company, (b) state the company's expectation of personnel, business partners and other parties linked to its operations, (c) are publically available and communicated internally and externally, (d) are embedded "throughout the company" and (e) are assessed by an independent third party firm.

- If the internal company policies do not meet the GOFA requirements outlined above, the company is required to explain why its policies do not meet the applicable requirement(s).
- If the company collects, obtains or stores personally identifiable information, or electronic or wire communications, it must disclose the details of any company policies addressing how the company will respond to requests by governments of Internet restricting countries for disclosure of such information.
- If the company provides an Internet search engine or an Internet content hosting service, the company must disclose all steps taken to provide users with clear, prominent and timely notice when content has been removed or blocked at the request of the Internet restricting country.¹⁷
- Bans on the Export of Internet Censoring and Surveillance Items to Internet Restricting Countries. A ban would be imposed on the export of certain goods or technology to "**government end users**" of Internet restricting countries if such goods or technology have been designated by the Secretary of Commerce as having the primary purpose of assisting in censorship or surveillance of telecommunications (including the Internet).¹⁸

Practical Impact of GOFA

– State Department Reports and Designations

GOFA's country reporting requirements proposed for the U.S. Secretary of State will likely cause additional headaches for embassy staff and the U.S. State Department - with the offsetting benefit of providing some embarrassment for regimes that are found to have engaged in censoring or monitoring activities. But, standing alone, these proposed reports do not break new ground. The Foreign Assistance Act of 1961, as amended, already requires the State Department to prepare Country Reports on Human Rights Practices for Congress.¹⁹ GOFA, among other things, would simply require those Country Reports to now address any Internet restricting practices of a country.

There is also precedent for GOFA's requirement that the Secretary of State annually designate Internet restricting countries. For instance, the International Religious Freedom Act of 1998, as amended, requires the President, on an annual basis, to designate as a "Country of Particular Concern" any country that has engaged in or tolerated particularly severe violations of religious freedom.²⁰ The President has delegated this designation obligation to the Secretary of State.²¹

Even in the absence of GOFA, the Executive Branch and the State Department have begun taking baby steps in expanding their engagement with "cyber" issues in foreign countries. On February 22, 2011, Christopher Painter was appointed as the State Department's Coordinator of Cyber Issues.²² In May of

2011, the Obama Administration announced its “International Strategy for Cyberspace”. As part of this announced strategy, the Administration indicated that the “United States will be a tireless advocate of fundamental freedoms of speech and association through cyberspace[.]”²³

– Export Bans

GOFAs proposed export restrictions are also evolutionary rather than revolutionary. The existing Export Administration Act of 1979, as amended (the “EAA”), and the Export Administration Regulations (the “EAR”) implementing the EAA, contain restrictions and prohibitions on the export of certain types of goods and technology.²⁴ The Foreign Asset Control Regulations (commonly referred to as “OFAC” regulations) also impose a number of restrictions on exporting items to certain persons and countries.

It is beyond the scope of this article to address in any level of detail the notoriously complex EAR rules. Nonetheless, two basic facts about the EAR should be noted. First, the EAR export restrictions applicable to particular exports depend on the item being exported, the country the item is being exported to, the user of the item and the use to which the item is to be put. Second, under the existing EAR rules, any U.S. origin electronic device, mechanical device, or other device, and any software related to such devices, “primarily useful for the surreptitious interception of wire, oral, or electronic communications” cannot be exported outside the U.S. in any event without a license issued by the Commerce Department’s Bureau of Industry and Security.²⁵

OFAC regulations in some cases go much farther than the restrictions imposed in the EAR. Indeed, subject to limited exceptions, OFAC regulations effectively prohibit any trade with the governments of certain suspect countries, such as Iran.²⁶

Admittedly, the export bans contained in GOFAs will apply to **any** government end users of “Internet restricting countries” as designated by the Secretary of State. That list would likely be larger than the list of countries subject to some of the most restrictive existing controls of OFAC and EAR. But in terms of the actual compliance practices, under GOFAs U.S. exporters will simply have to add a new step in their (hopefully) already existing export compliance procedures.

– New Public Filing Requirements

As a practical matter, GOFAs most onerous requirement is likely to be the new proposed public filing requirements. On their face, the requirements only apply to “Internet communications service companies” operating in Internet restricting countries and whose securities publicly trade in the U.S. At first glance, this public filing requirement would appear to have very limited reach and only apply to publicly traded internet service providers (“ISPs”) or perhaps web portal companies like Yahoo or Google. In fact, the public filing requirements have much broader impact.

GOFAs defines “Internet communications service companies” fairly expansively to include any company that

“(i) is required to file an annual report with [the Securities Exchange Commission]; and

(ii)(I) provides *electronic communication services* or *remote computing services*; or

(II) is a domain name registrar, domain name registry, or other domain name registration authority”²⁷ (emphasis added).

In turn, an “electronic communications service” is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.”²⁸ A “remote computing service” is defined as the provision to “the public of computer storage or processing services by means of an electronic communications system.”²⁹ Each of these definitions creates difficulties for publicly traded companies.

Under a literal reading of the proposed legislation, if a multinational corporation with offices in an Internet restricting country provides phones, email access or fax machines to its employees or contractors in that Internet restricting country, that company would likely be deemed to be providing an “electronic communication service.” GOFAs does not appear to contain any limitation that the “electronic communication service” be provided for a fee or offered to the public.

The definition of “remote computing service” would cover cloud computing services or website hosting services provided to the public at large by a company. Arguably, a publicly traded company offering cloud computing service or website hosting services could be subject to GOFAs filing requirements, even if its servers are exclusively located in the U.S., so long as the services could be used by members of the public in an Internet restricting country.

Foreign corporations would also not be immune from GOFAs reach if their securities publicly trade in the U.S. and they are subject to filing periodic reports with the SEC. Prominent foreign outsourcing companies like Infosys Technologies Limited and Wipro Limited, whose securities trade in the U.S. and who are required to make periodic filings with the SEC, could find themselves subject to GOFAs.

If subject to GOFAs filing requirements, a company, among other things, would be required to develop a human rights policy “that mirrors the Guidelines for Multinational Enterprises issued by the Organization for Economic Co-Operation and Development[.]”³⁰ This policy would need to be publicly communicated to – and set forth the company’s expectation of – its employees, business partners, contractors and vendors.³¹ A vendor who provides an outsourced service to a company subject to GOFAs filing requirements could effectively find itself subject to GOFAs.

Prospects for GOFA's Passage

It is difficult to predict whether the current Congress will pass GOFA in some form. There have been previous versions of GOFA that were introduced in earlier Congressional sessions. Following Congressional hearings in February of 2006, Congressman Smith introduced the Global Online Freedom Act of 2006, but the Congressional term ended without the Bill's passage.³² The Global Online Freedom Act of 2007 fared better with the 110th Congress and successfully made its way through three committees before it died.³³ It remains to be seen whether there is enough popular support to pass the Global Online Freedom Act of 2011.

Final Thoughts

There are abundant examples of government actors in many states using the internet to monitor and repress the expression of their citizens. More disturbingly, it appears that at least some U.S. and European companies are trying to market and distribute the tools of repression. Yet, it is not at all clear that laws such as GOFA will materially deter or stop governments from censoring or monitoring their citizens, but such laws will undoubtedly create new compliance burdens on many multinational enterprises.

Todd Taylor is a Senior Counsel in Moore & Van Allen PLLC's Intellectual Property practice group and its Commercial & Technology Transactions practice group. Todd's practice is focused on Ecommerce, technology, outsourcing, and supply chain matters. Over his sixteen years as a practicing lawyer he has worked extensively on various corporate, technology licensing, cross-border and third party servicing matters.

¹ The Global Online Freedom Act of 2011, H.R. 3605, 112th Cong. (2011).

² *Promoting Global Internet Freedom: Hearing Before the Subcomm. on Africa, Global Health and Human Rights of the H. Comm. on Foreign Affairs*, 112th Cong. (2011) (excerpts of statement of Rep. Chris Smith, Chairman of H. Subcomm. on Africa, Global Health and Human Rights), http://chrissmith.house.gov/UploadedFiles/2011_12_08_GOFA_hearing.pdf.

³ Comment by Russian MFA Spokesman Alexander Lukashevich Regarding Consideration in US Congress of New Global Online Freedom Act (Dec. 19, 2011),

http://www.mid.ru/bdomp/Brp_4.nsf/arh/6E3B1A3D5A15F5114425796C002DCD96?OpenDocument.

⁴ Philip N. Howard, Sheetal D. Agarwal, and Muzammil M. Hussain, *The Dictators' Digital Dilemma: When Do States Disconnect their Digital Network?* Issues in Tech. Innovation (Ctr. For Tech. Innovation at Brookings), Oct. 2011 at 1, available at http://www.brookings.edu/~media/Files/rc/papers/2011/10_dictators_digital_network/10_dictators_digital_network.pdf.

⁵ *Id.* at 6.

⁶ See *A Global Assessment of Internet and Digital Media*, Freedom on the Net 2011 (Freedom House, April 18, 2011) at 23, <http://www.freedomhouse.org/images/File/FotN/FOTN2011.pdf>.

⁷ See *id.* at 26.

⁸ See *id.* at 27.

⁹ See *id.*

¹⁰ See Ben Elgin, Vernon Silver and Alan Katz, *Iranian Police Seizing Dissidents Get Aid of Western Companies*, Bloomberg News (Oct. 30, 2011).

¹¹ See *A Global Assessment of Internet and Digital Media*, *supra* note 6, at 16.

¹² See Vernon Silver, *Post-Revolt Tunisia Can Alter E-Mail with "Big Brother" Software*, Bloomberg News (Dec. 12, 2011).

¹³ See Ben Elgin and Vernon Silver, *U.S. Calls for NetApp Probe on Syria Spy Tech*, Bloomberg News (Nov. 10, 2011).

¹⁴ See *Iranian Police Seizing Dissidents Get Aid of Western Companies*, *supra* note 10.

¹⁵ See Global Online Freedom Act of 2011 § 103.

¹⁶ See *id.* § 104.

¹⁷ See *id.* § 201.

¹⁸ See *id.* § 301.

¹⁹ See 22 U.S.C. § 2151n(d); 22 U.S.C. § 2304(b).

²⁰ See 22 U.S.C. § 6442(b).

²¹ See Memorandum of August 17, 1999: Delegation of Responsibilities Under the International Religious Freedom Act of 1998, 64 Fed. Reg. 47,345 (Aug. 17, 1999).

²² See Press Release, Office of the Spokesman of the U.S. Dept. of State, Appointment of Christopher Painter as Coordinator for Cyber Issues (April 11, 2011), <http://www.state.gov/r/pa/prs/ps/2011/04/161485.htm>.

²³ President Barack Obama, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World 24 (2011), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

²⁴ See, e.g., 50 U.S.C. app. § 2405(a)(1) and 15 C.F.R. § 736(2)(b).

²⁵ 15 C.F.R. § 742.13.

²⁶ See, e.g., 31 C.F.R. Part 560.

²⁷ Global Online Freedom Act of 2011 §201(a).

²⁸ 18 U.S.C. § 2510(15).

²⁹ 18 U.S.C. § 2711(2).

³⁰ Global Online Freedom Act of 2011 §201(a).

³¹ See *Id.*

³² See History of H.R. 4780 <http://www.gpo.gov/fdsys/search/pagedetails.action?browsePath=109%2FHR%2F%5B4700%3B4799%5D&granuleId=HOB-2006-hr4780&packageId=HOB-2006&fromBrowse=>. See also Robert McMahon and Isabella Bennett, *U.S. Internet Providers and the Great Firewall of China*, Background (Council on Foreign Relations, Feb. 23, 2011), <http://www.cfr.org/china/us-internet-providers-great-firewall-china/p9856#>.

³³ See McMahon and Bennett, *supra* note 32.