

2012

## Good for the Bottom Line: Incentivizing Private Companies to Join the Global Network Initiative

Arielle Joy Albert

Follow this and additional works at: <https://scholarlycommons.law.hofstra.edu/jibl>



Part of the [Law Commons](#)

---

### Recommended Citation

Albert, Arielle Joy (2012) "Good for the Bottom Line: Incentivizing Private Companies to Join the Global Network Initiative," *Journal of International Business and Law*. Vol. 11: Iss. 2, Article 8.

Available at: <https://scholarlycommons.law.hofstra.edu/jibl/vol11/iss2/8>

This Notes & Student Works is brought to you for free and open access by Scholarship @ Hofstra Law. It has been accepted for inclusion in Journal of International Business and Law by an authorized editor of Scholarship @ Hofstra Law. For more information, please contact [lawscholarlycommons@hofstra.edu](mailto:lawscholarlycommons@hofstra.edu).

## GOOD FOR THE BOTTOM LINE: INCENTIVIZING PRIVATE COMPANIES TO JOIN THE GLOBAL NETWORK INITIATIVE

Arielle Joy Albert\*

### INTRODUCTION

There is an ongoing debate concerning whether a police power should exist over domestic Information and Communication Technology (ICT) companies that comply with foreign Internet laws that violate a user's rights of privacy and expression on the Internet.<sup>1</sup> While the introduction of the Internet has created endless possibilities for its users, it has also created numerous opportunities for foreign countries to invade the rights of citizens.<sup>2</sup> In response to these violations, public and private remedies have developed seeking to limit the ways in which a foreign government can use the Internet to invade the rights of individuals.<sup>3</sup>

This Note proposes that the Global Network Initiative (GNI) is the preeminent solution among all remedies offered privately and publicly that address ICT compliance with foreign censorship laws. Thus, it is imperative that the federal government and members of the ICT community assist the GNI in attaining the level of compliance necessary to be effective.

Part II of this Note describes the manner in which foreign governments rely on private ICT companies to comply with strict Internet laws that often violate a user's rights of privacy and expression on the Internet.<sup>4</sup> These foreign laws require ICT companies to deactivate user accounts, provide governments with products that enable censorship, restrict products that circumvent regulations, and provide access to personal information.<sup>5</sup> Part II of this Note will also address the human rights implications engendered in ICT compliance including

---

\* I would like to thank, first and foremost, my family- my fiancé Neil for his unwavering love and support over the last six years; my sister for constantly reminding me that attaining success is never easy but that the sweetest victories are those worked hardest for; to my mother for instilling in me the ambition and confidence necessary to realize my dreams; to Joe for his constant support; and last, but certainly not least, my father for always encouraging me to value the past, live in the moment and trust my instincts. I would like to thank Professor Frank Gulino for his guidance and insight throughout the writing process as well as the editorial board and staff members of the *Journal for International Business and Law*. I give special thanks to my friends for supporting and advising me throughout the writing process. And, finally, I dedicate this note to all the individuals and institutions- especially the Global Network Initiative- for fighting to make the Internet a place where all individuals can express themselves freely.

<sup>1</sup> See John Palfrey, *Four Phases of Internet Regulation*, 77 SOC. RESEARCH 3, 15 (2010).

<sup>2</sup> See DUNSTAN A. HOPE, PROTECTING HUMAN RIGHTS IN THE DIGITAL AGE: UNDERSTANDING EVOLVING FREEDOM OF EXPRESSION AND PRIVACY IN THE INFORMATION AND COMMUNICATIONS TECHNOLOGY INDUSTRY 1, 4 (2011), [http://www.bsr.org/reports/BSR\\_Protecting\\_Human\\_Rights\\_in\\_the\\_Digital\\_Age.pdf](http://www.bsr.org/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf). Not all Internet regulations violate a user's rights of privacy and expression. See *id.* at 6. There are legitimate reasons why a government may choose to restrict content on the Internet or require private companies to disclose or restrict information. *Id.* For instance, Governments may lawfully remove images of child pornography or request access to personal information in order to investigate acts of "fraud, terrorism or other violent crimes". *Id.*

<sup>3</sup> See PATRICIA M. FIGLIOLA ET AL, CONG. RESEARCH SERV. R41120, U.S. INITIATIVES TO PROMOTE GLOBAL INTERNET FREEDOM: ISSUES, POLICY AND TECHNOLOGY 1, 16-17 (2011) [hereinafter CRS].

<sup>4</sup> See Hope, *supra* note 2, at 1.

<sup>5</sup> *Id.* at 19.

the harassment, detainment and wrongful death of Internet users in countries like China, Iran and Egypt pursuant to such laws.<sup>6</sup> In addition, Part II will highlight the tough choices ICT companies face in conducting business in foreign countries and complying with such laws, while also attempting to protect human rights.<sup>7</sup>

The choice between business and morality may appear uncomplicated. However, the economic consequence of rejecting a country's demand to censor the Internet weighs heavily on most ICT companies.<sup>8</sup> Despite the inherent legal issues associated with monitoring domestic ICT firms abroad, the pressure for control over these companies is mounting as acts of violence against private individuals and violations of their rights to expression and privacy on the Internet escalate.<sup>9</sup>

Part III of this Note will trace the efforts made by private entities like the GNI and governmental entities to regulate the compliance of ICT companies with foreign censorship laws that violate citizens' rights of expression and privacy. The United States government has attempted to hold ICT companies liable for acts of violence arising out of its compliance with censorship laws.<sup>10</sup>

While ICT community members, scholars and government representatives have proffered a number of possible solutions aimed at addressing ICT complicity, these proposals have not been effective for numerous reasons.<sup>11</sup> Part III of this Note will articulate certain barriers faced by government solutions, including jurisdictional constraints and economic con-

---

<sup>6</sup> See CRS, *supra* note 3, at 4, 10; *infra* text accompanying note 52.

<sup>7</sup> See Luke Allnut, *Vodafone in Egypt: How Tech Companies Can Uphold, not Violate Human Rights*, THE CHRISTIAN SCIENCE MONITOR 1, 2 (Feb. 22, 2011), <http://www.csmonitor.com/Commentary/Opinion/2011/0222/Vodafone-in-Egypt-How-tech-companies-can-uphold-not-violate-human-rights/%28page%29/2> ("Upholding a certain government's policies puts companies in local compliance, but can also conflict with international standards for human rights"). ICT companies may also be held criminally liable for complying with policies that violate users' rights even if they are in local compliance. See Bill Lambrect, *Tech Firms that Abet Censors Face Threat*, ST. LOUIS POST-DISPATCH, at A1, Mar. 4, 2010.

<sup>8</sup> See Su Zhen, *U.S. Internet Companies Human Rights Initiative Expert Review Full of Empty Text*, EPOCHTIMES (Taiwan), Nov. 4 2008, <http://translate.google.com/translate?hl=en&langpair=zh-TW—en&u=http://www.epochtimes.com/b5/8/11/4/n2319531.htm>. Despite moral considerations, many companies "seem ready to stop at nothing to conquer new markets" and companies such as "Bull, Nokia, Bluecoat, Netfirms and Cisco have all yielded to the lure of profits". See also Nabeel Rajab, *Reporters Without Borders: the Need to Impose Sanctions on Companies*, REPORTERS WITHOUT BORDERS (Feb. 2, 2011) [http://arabia.reporters-sans-frontieres.org/imprimer\\_ar.php3%3Fid\\_article%3D32095](http://arabia.reporters-sans-frontieres.org/imprimer_ar.php3%3Fid_article%3D32095).

<sup>9</sup> See Lambrect, *supra* note 7 (highlighting Sen. Richard Durbin's [D-IL] threat to draft legislation that will impose criminal penalties against ICT companies that comply with censorship abroad); Hillary Rodham Clinton, U.S. Sec'y of State, Secretary Of State Hillary Rodham Clinton Delivers Remarks On Internet Freedom At The Newseum- Part 2 (Jan. 21, 2010), available at 2010 WLNR 1304706 [hereinafter Clinton] (announcing the federal government's recommitment to promoting freedom of speech and privacy online and calling on companies to act morally and secure the trust of internet users abroad).

<sup>10</sup> See *Lawyers and legislators put pressure on globe-trotting tech firms*, THE ECONOMIST (Jul. 21st 2011), <http://www.economist.com/node/18986482> [hereinafter, *Lawyers and legislators*]. The United States government has tried to impose liability on ICT companies under the 1789 Alien Tort Statute (also known as the Alien Tort Claims Act) or the Global Online Freedom Act (GOFA) which was introduced to Congress in 2006 but has not been passed. See *id.*

<sup>11</sup> See generally Jessica E. Bauml, *It's a Mad, Mad Internet: Globalization and the Challenges Presented By Internet Censorship*, 63 FED. COMM. L.J. 697, at 710 (2011) (detailing the history on Internet censorship and reviewing the private and government solutions provided but ultimately concluding that no solution may be appropriate since they all offend the notion of comity between nations).

GOOD FOR THE BOTTOM LINE

cerns.<sup>12</sup> Further, Part III will also address the reasons why the strict regulations that would be imposed by Federal legislation make it unlikely that a governmental solution will be effective in monitoring the conduct of ICT companies abroad.<sup>13</sup>

Part IV of this Note describes the unique structure of the GNI. The GNI is a private organization founded in 2008 by Google, Yahoo! and Microsoft.<sup>14</sup> The GNI employs similar values to those espoused in GOFA; however, adoption of the GNI's Principles does not carry the same weight of legal liability.<sup>15</sup> The GNI seeks to assemble uniform policies within the ICT community that ICT companies will uphold when operating in countries that limit and surveil the Internet.<sup>16</sup>

Part V of this Note will set forth the reasons why the GNI is the most viable solution. Under the GNI's Framework, member companies would not need to choose between business and morality but would be responsible for upholding the GNI policies when complying with government demands.<sup>17</sup> The GNI's policies aim to provide "high-level guidance" to the ICT community on respecting and protecting users' rights of privacy and expression while also respecting a company's choice to conduct business abroad. Because it would be impracticable to prohibit ICT companies from operating in countries with strict Internet laws, the GNI instead seeks to create "sustainable solutions" within the ICT community that will make the Internet safer for users.<sup>18</sup>

Part V of this Note will also address the difficulties faced by the GNI in protecting the rights of expression and privacy on the Internet. Despite the ability of GNI members to "self-regulate" and maintain business in countries with strict Internet laws, ICT companies are reluctant to join the organization.<sup>19</sup> A paramount concern of ICT companies is the cost associated with upholding the GNI's Principles.<sup>20</sup> The costs incurred by ICT companies, especially those not as large as Google, Yahoo!, and Microsoft are high as compliance requires

---

<sup>12</sup> See *id.* at 716.

<sup>13</sup> See *id.*

<sup>14</sup> See *Protecting and Advancing Freedom of Expression and Privacy in Information and Communications Technologies*, ANNIVERSARY NEWSLETTER 1 (Global Network Initiative New York, N.Y.), 2009, available at (<http://globalnetworkinitiative.org/http://www.globalnetworkinitiative.org/newsletter/index.php>) [hereinafter ANNIVERSARY NEWSLETTER].

<sup>15</sup> See Bauml, *supra* note 11, at 719 (noting the shared similarities between the GNI and the Global Online Freedom Act but also recognizing that the GNI is the better solution because it "tackle[s] the critical issues inherent in GOFA"). The GNI does not forbid ICT companies from complying with laws that may violate rights of expression and privacy. *Id.* at 720.

<sup>16</sup> See GLOBAL NETWORK INITIATIVE, PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY 1 (2008), <http://www.globalnetworkinitiative.org/principles/index.php> [hereinafter PRINCIPLES] ("Information and Communications Technology (ICT) companies have the responsibility to respect and protect the freedom of expression and privacy rights of their users. . . [and to] enable the exchange of ideas and access to information in a way that supports economic opportunity, advances knowledge and improves quality of life.").

<sup>17</sup> See *id.* At 4 (participating companies must make a "good faith" effort to implement to GNI Principles).

<sup>18</sup> See GLOBAL NETWORK INITIATIVE, GOVERNANCE, ACCOUNTABILITY AND LEARNING FRAMEWORK (2008), available at <http://www.globalnetworkinitiative.org/governanceframework/index.php> [hereinafter GNI, ACCOUNTABILITY FRAMEWORK].

<sup>19</sup> See Larry Downes, *Why no one will join the Global Network Initiative*, FORBES (Mar. 30, 2011, 12:20), <http://www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/>. There are currently 31 members of the GNI but only a fraction of those members are ICT companies. *Participants*, THE GLOBAL NETWORK INITIATIVE (2012), <http://www.globalnetworkinitiative.org/participants/index.php>.

<sup>20</sup> See Downes, *supra* note 19.

member companies to dedicate employee time that may not be readily available.<sup>21</sup> Economic concerns are compounded by the belief of ICT companies that they can protect the rights of Internet user's in-house.<sup>22</sup>

Since the GNI does not have the ability to enforce its policies legally, the organization has relied on companies to voluntarily become members and comply with its Principles. However, the economic concerns associated with membership have hindered enrollment and thus limit the effectiveness of the GNI.<sup>23</sup> Requirements of the GNI, such as the requirement that ICT companies create an internal compliance department, highlight the need for the organization to find ways to mitigate the financial loss caused to companies that join. Notwithstanding the complications faced by the GNI it remains the most viable solution today and efforts should be made by the GNI as well as the United States government to give the organization the opportunity to be successful.

This Note will conclude by proposing that federal money be allocated to the GNI in order to limit the cost of participation. In addition to financial support this Note calls on the United States government to direct its energy away from legislative remedies and publicly support the GNI as the paramount solution. This Note also proposes that it would be in the best interest of the GNI if its founding members, Goggle, Yahoo! and Microsoft, dedicate financial support and advertising support for new members in order to entice enrollment.

## II. COUNTRIES WITH OPPRESSIVE INTERNET LAWS USE ICT COMPANIES TO CENSOR THE INTERNET, RESULTING IN VIOLATIONS OF A USER'S RIGHTS OF EXPRESSION AND PRIVACY

The Internet has evolved into a "world where vast Information and Communications Technology (ICT) infrastructures and extensive flows of information have become natural and unquestioned features of modern life."<sup>24</sup> However, the introduction of the Internet has also created numerous opportunities for countries to invade the rights of their citizens. Foreign governments and private ICT companies share a dependent relationship in which most governments rely on private ICT companies to surveil and limit content on the Internet and private ICT companies depend on foreign governments for a source of revenue.<sup>25</sup> Human rights, specifically rights of expression and privacy, are continually implicated when ICT companies cede to government demands to restrict access to the Internet or provide governments with user information.<sup>26</sup>

---

<sup>21</sup> *See id.*

<sup>22</sup> *See* Verne G. Kopytoff, *Sites Like Twitter Absent From Free Speech Pact*, N.Y. TIMES, Mar. 7, 2011, at B4.

<sup>23</sup> *See id.*

<sup>24</sup> Hope, *supra* note 2, at 8.

<sup>25</sup> *See id.* at 4 (explaining how foreign governments rely of ICT companies to censor the internet); *See* Elizabeth M. Lynch, *This is Not Your Daddy's China— Or Is It?*, CHINA LAW & POLICY (Nov. 24, 2011), <http://chinalawandpolicy.com/tag/chinas-internet-censorship/>. Companies who reject Chinese censorship laws are not permitted to conduct business in the country but companies that "do their job well don't just stay in business, but are rewarded for their vigilant censorship". *See id.*

<sup>26</sup> The Universal Declaration for Human Rights protects the right to privacy and freedom of expression and ICT companies must protect those rights as the functions of the Internet and technology continue to evolve. *See* Hope, *supra* note 2, at 5.

GOOD FOR THE BOTTOM LINE

**A. Oppressive Internet Laws Have Led to the Harassment, Detainment, and Death of Internet Users**

China is the leading example of a foreign country that censors the Internet.<sup>27</sup> Not only does China have “one of the most sophisticated and aggressive Internet Censorship and control regimes in the world,” but they also make up the world’s largest Internet-using population.<sup>28</sup> The Chinese government blocks a number of websites, including Facebook, Twitter and YouTube, and uses a variety of methods to limit Internet content and user expression.<sup>29</sup>

Chinese censorship policies have resulted in numerous human right violations. Many of these violations are the result of ICT compliance with Chinese Internet laws.<sup>30</sup> Over the years, several Chinese journalists have been detained for providing “state secrets” over the Internet.<sup>31</sup>

For example, Shi Tao is a Chinese journalist currently serving ten years in prison for illegally providing state secrets via his personal Yahoo! e-mail account.<sup>32</sup> The detention of Shi Tao was based on information provided by Yahoo! to the Beijing State Security Bureau in response to a request for information from Mr. Tao’s e-mail account.<sup>33</sup> The Beijing State Security Bureau requested a multitude of information from Yahoo! concerning Mr. Tao, including personal information used to register for the e-mail account, e-mail login times, and associated Internet Protocol (IP) addresses used to access his Yahoo! e-mail account.<sup>34</sup> The reason provided by the Beijing State Security Bureau for this request was Mr. Tao’s “illegal provision of state secrets to foreign entities.”<sup>35</sup> However contrary to the reason cited by the Beijing State Security Bureau, alternative records indicate that Mr. Tao’s arrest was premised

---

<sup>27</sup> See *Internet Censorship in China*, N.Y. TIMES, (Mar. 22, 2010), [http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet\\_censorship/index.html](http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html); CRS, *supra* note 3, at 4. The Chinese government uses “website blocking and keyword filtering” to control Internet content and expression. *Id.* at 5. They control the Internet by “regulating and monitoring Internet service providers, Internet cafes, and university bulletin board systems [and] registering websites and blogs”. See *id.* China has been notorious for arresting “cyber dissidents” and shutting down Internet service providers for not complying with the Internet laws. *Id.*

<sup>28</sup> CRS, *supra* note 3, at 4; See *Global Internet Freedom: Corporate Responsibility and the Rule of Law* (Human Rights in China, New York, N.Y.) available at <http://www.hrichina.org/content/4047>.

<sup>29</sup> See CRS, *supra* note 3, at 5. China blocks many social networking and alternative news websites including “Radio Free Asia, international human rights websites, many Taiwanese newspapers, Facebook, Twitter, and YouTube”. *Id.* The Chinese government “reportedly has hired thousands of students to express pro-government views on websites, bulletin boards, and chat rooms.” *Id.*

<sup>30</sup> See Rebecca MacKinnon, *Shi Tao, Yahoo!, and the lessons for corporate social responsibility*, (Journalism & Media Studies Centre, University of Hong Kong, Working Paper No. 1.0, 2007) available at <http://rconversation.blogs.com/YahooShiTaoLessons.pdf> [hereinafter MacKinnon, Working Paper]

<sup>31</sup> See *id.*; CRS, *supra* note 3, at 4 (estimating that “between 30 and 40 Chinese citizens are serving prison sentences for writing about politically sensitive topics online”). Chinese officials have defended Internet regulations and argue that Internet controls are necessary for social stability and that new restrictions target “harmful content” such as pornography. See *id.*

<sup>32</sup> Rebecca MacKinnon, *the Shi Tao case, and lessons for corporate social responsibility*, RCONVERSATION (Jan. 3, 2008), <http://rconversation.blogs.com/rconversation/2008/01/yahoo-the-shi-t.html> [hereinafter MacKinnon, Blog]. Shi Tao was detained on November 24, 2004 and sentenced in 2005 to ten years in prison for illegally providing state secrets via the Internet. *Id.*

<sup>33</sup> See *id.*

<sup>34</sup> See MacKinnon Working Paper, *supra* note 30.

<sup>35</sup> See Thomas Claburn, *Yahoo Testimony About Imprisoned Reporter Contradicted*, INFORMATIONWEEK (July 30, 2007), <http://www.informationweek.com/news/201201833>.

## THE JOURNAL OF INTERNATIONAL BUSINESS &amp; LAW

on an e-mail he had sent to a U.S. website, “Democracy Forum,” discussing security preparations being made for the fifteenth anniversary of the Tiananmen Square protests.<sup>36</sup>

Though Internet censorship is pervasive in China, it is not the only country with laws that stifle Internet freedom. Censorship is widespread and is often used as a mechanism to control citizens in many countries.<sup>37</sup> China, Iran and Egypt are just three of many countries that limit use of the Internet.<sup>38</sup>

The Iranian government has policies similar to the policies in China. The policies in Iran limit the use of the Internet, especially access to social networking web sites used by activists and bloggers.<sup>39</sup> Iranian cybercafés are required to record all websites visited by patrons and maintain video documentation of patrons for at least six months.<sup>40</sup> Additionally, Internet users must provide cybercafés with personal information “such as their name, father’s name, national ID number, and telephone number” in order to access the Internet.<sup>41</sup> The Iranian government also controls the Internet by limiting the speed of Internet access that ICT companies can provide to households, inhibiting users’ ability to access multimedia content.<sup>42</sup>

Like China, Iran has not hesitated to arrest journalists and bloggers for neglecting to abide by the country’s strict Internet policies. Reporters Without Borders stated that “in 2009, more than 200 Iranian journalists and bloggers were arrested and incarcerated in Iran . . . refer[ing] to Iran as the biggest jail for journalists in the Middle East.”<sup>43</sup> The effect of Iranian Internet censorship goes beyond the detention of journalists. The Iranian government has also been accused of harassing and arresting family members of those who violate Iranian Internet laws.<sup>44</sup>

Along with China and Iran, Internet censorship is practiced in Egypt as well and was employed during the 2011 Egyptian protest against former president Hosni Mubarak.<sup>45</sup> During the 2011 protests, former President Mubarak ordered the Internet to be shut down by invoking the “emergency powers of [Egypt’s] Telecommunications Act” which forced all providers to cut both mobile access and Internet access.<sup>46</sup> ICT companies operating in Egypt at the time, including “all of the major [Internet Service Providers] in Egypt, [such as]

<sup>36</sup> See MacKinnon, Blog, *supra* note 32.

<sup>37</sup> See CRS, *supra* note 3, at 4 (listing “China, Cuba, North Korea, Belarus, Myanmar, Egypt, Ethiopia, Iran, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, Vietnam, and Zimbabwe” as the top 15 countries using Internet restrictions that may violate a users right to freedom on the Internet).

<sup>38</sup> See *id.*

<sup>39</sup> See Golnaz Esfandiari, *Iran Announces New Restrictions For Internet Cafes*, RADIO FREE EUROPE RADIO LIBERTY (January 4, 2012), [http://www.rferl.org/content/iran\\_announces\\_new\\_internet\\_restrictions/24442396.html](http://www.rferl.org/content/iran_announces_new_internet_restrictions/24442396.html).

<sup>40</sup> *Id.*

<sup>41</sup> *Id.*

<sup>42</sup> See CRS, *supra* note 3, at 10.

<sup>43</sup> Radio Zamaneh, *Iran Arrests Four Journalists*, EURASIA REVIEW (Oct. 7, 2011), <http://www.eurasiareview.com/07102011-iran-arrests-four-journalists/>.

<sup>44</sup> See CRS, *supra* note 3, at 10.

<sup>45</sup> Eva Galperin, *Egypt’s Internet Blackout Highlights Danger of Weak Links, Usefulness of Quick Links*, ELECTRONIC FRONTIER FOUNDATION, (Feb. 8, 2011), <https://www EFF.org/deepinks/2011/02/egypts-internet-blackout-highlights-danger-weak>.

<sup>46</sup> See Sandra Louven & Catherine Slodczyk, *As Despots Spoon- the mobile communications*, HANDELSBLATT (April 2, 2011, 16:03), <http://translate.google.com/translate?hl=en&langpair=de—en&u=http://www.handelsblatt.com/unternehmen/it-medien/wie-despoten-die-mobilfunk-er-gaengeln/3823692.html%3Fp3823692%3Dall>. (Ger.)

GOOD FOR THE BOTTOM LINE

Vodafone, Telecom Egypt, Etisalat Misr, and Internet Egypt Network took their services offline within minutes of each other” and U.S. companies like Facebook and Twitter were dis-banded.<sup>47</sup> While many of the ICT companies operating in Egypt at the time issued statements declaring disapproval of the Internet shut down, they explained the “dead end” situation they were placed in, forcing them to inevitably comply with Egypt’s request.<sup>48</sup> For example, Vodafone claimed that, “had they refused [to shut down the internet and mobile networks] the management could have been arrested on the spot.”<sup>49</sup>

While activists have been able to circumvent Egypt’s tight grasp on the Internet, there are still victims of the country’s strict Internet policies- most notably Egyptian citizen Khaled Said.<sup>50</sup> In the summer of 2009, Mr. Said was “dragged out of an Internet café” and beaten to death by the Egyptian police in retaliation for a blog post that reflected poorly on the Egyptian Police Department.<sup>51</sup> Although unconfirmed, it has been suggested that Egypt’s strict Internet policies required the ICT provider involved to disclose information that allowed the Egyptian police to track and locate Mr. Said.<sup>52</sup>

**B. Governments Use ICT Companies to Censor the Internet Because They Do Not Have the Capabilities to Control the Internet Directly**

Incidents like the arrest of Shi Tao in China and the death of Khaled Said in Egypt highlight the difficult position ICT companies are placed in when asked to divulge the personal information about their users and limit Internet content. Activists are reluctant to accept the difficult position described by ICT companies as an “excuse.”<sup>53</sup> Despite the concerns of activists, private ICT companies have consistently served as a vehicle for governments to

<sup>47</sup> See Galperin, *supra* note 45.

<sup>48</sup> See Louven & Slodczyk, *supra* note 45.

<sup>49</sup> See *id.* Vodafone was also responsible for sending pro- Mubarak text messages during the 2011 protest. *Id.*

<sup>50</sup> Anne Alexander, *Internet role in Egypt’s protests*, BBC (Feb. 9, 2011), <http://www.bbc.co.uk/news/world-middle-east-12400319> (referencing the death of Khaled Said). The Egyptian government has set up a “special unit to monitor Internet activists” however Internet users have circumvented Internet controls by organizing on social media websites like Facebook. See *id.* Activist use of Facebook to politically organize has been the protagonist to government demands to shut down the Internet and take Facebook offline. See *id.*

<sup>51</sup> See Sunday Morning Revelations, *Khaled Said*, TUBLR (Feb. 2, 2011) <http://sundaymorningrevelations.tumblr.com/post/3081418731/khaled-said> (“On that summer day of June 6th 2009, Khaled stumbled upon a group of police men who were dealing out the drugs that they had confiscated from someone. . .Khaled didn’t say anything. . . but instead chose to tell the world what had happened through his blog”).

<sup>52</sup> See *id.* (“The police might have had an Internet content screen for anything that was published in Egypt with the word ‘police’ in it, because a couple of hours later, 2 un-uniformed officers set out to find Khaled. The search was short; they found him at an Internet café just a couple minutes away from his home. Upon being sighted, Khaled was forcefully moved away from the establishment. . . 20 minutes later, he was dead”). The Egyptian laws pertaining to Internet use have been escalating, “in February 2005, Egypt’s Ministry of Interior ordered Internet café managers and owners to record their customers’ names and ID numbers and threatened to close the cafés if they refused to comply” and “[i]n August 2008, Egyptian authorities increased the level of Internet surveillance by demanding that Internet café customers must provide their names, e-mail addresses, and phone numbers before they can use the Internet. *Internet Filtering in Egypt*, OPENNET INITIATIVE, 4 (2009), [http://opennet.net/sites/opennet.net/files/ONI\\_Egypt\\_2009.pdf](http://opennet.net/sites/opennet.net/files/ONI_Egypt_2009.pdf). Once the Internet café is provided the required information the “[c]ustomer will receive a text message on their cell phones with a pin number that they can use to access the Internet.” *Id.* See generally Alexander, *supra* note 50 (explaining how Mr. Said’s death was the catalyst for protests where citizens used the Internet to organize and skirt Internet regulations).

<sup>53</sup> See Galperin, *supra* note 45 (arguing that despite the difficult situations ICT’s face they should not be “off the metaphorical hook with the lame, dangerous excuse of ‘just following orders’” but that ICT’s need to



carry out Internet regulations.<sup>54</sup> Governments like China and Iran rely on private ICT companies because they do not have the capabilities to “implement the level of control they seek directly. . . . [Thus they turn] to private companies like Google to do most of the blocking or surveillance.”<sup>55</sup> As the Internet has evolved, governments have relied on ICT companies to deactivate user accounts, provide products that enable censorship, restrict products that circumvent regulations, and provide access to personal information.<sup>56</sup>

China and other censoring regimes create stringent Internet laws forcing ICT companies to comply with censorship policies or face a variety of consequences ranging from legal penalties to ceasing business operations in that country.<sup>57</sup> Many countries hold ICT companies liable “for user-generated content that is carried over their services, such as blogging sites and video hosting” which violate their censorship policies.<sup>58</sup> ICT companies’ fear of liability was exemplified in Vodafone’s compliance with Egypt’s Internet policies during the 2011 protest.<sup>59</sup> The fears of ICT companies operating in foreign countries have been further perpetuated by governments’ vague definitions of illegal content, leading companies to self-censor and restrain speech as a preemptive tactic to avoid liability.<sup>60</sup>

In addition to legal concerns many ICT companies are confronted with potential economic losses if they do not comply with demands to limit the Internet. Google’s 2010 showdown with the Chinese government (which resulted in Google’s continued compliance with Chinese censorship laws) is becoming a familiar scenario.<sup>61</sup> ICT companies must

---

recognize the responsibilities they have to the public and be more accountable for the “impact they have on human rights”).

<sup>54</sup> See generally Palfrey, *supra* note 1, at 2. The progression of ICT regulation can be identified in four phases; (1) Open Internet, from the birth of the internet through the year 2000, (2) Access Denied, from 2000-2005, (3) Access Controlled, from 2005-2010 and (4) the current phase, Access Contested. *Id.* During the “Open Internet” phase nation states approached the Internet as a separate cyberspace and regulation was not something seriously considered. *Id.* During Access Denied countries began viewing activities and expression on the Internet as something that required management and began implementing policies to monitor Internet content. *Id.* at 7-8. For example, certain countries began “filtering” information on the Internet. *Id.* A greater attempt to limit content was made during Access Controlled. *Id.* at 12-14. Many governments seeking to regulate the Internet realized the value ICT companies had during this period. See *id.* at 14. After experiencing difficulties in blocking and controlling the Internet though government run surveillance programs many countries began applying pressure on private ICT’s to limit and surveil the Internet. see *id.* Currently Internet regulation is in an Access Contested phase” where activist are attempting to get Internet companies to reject regulations previously implemented. *Id.* at 16. Activist argue that the difficulties presented to governments during the Access Denied period indicate that if private ICT’s do not regulate the Internet, oppressive regimes will face severe hardship in trying to carry out regulations themselves. See *id.* at 14.

<sup>55</sup> See *id.* at 14.

<sup>56</sup> See Hope, *supra* note 2, at 19-20.

<sup>57</sup> See Lynch, *supra* note 25.

<sup>58</sup> See Hope, *supra* note 2, at 19.

<sup>59</sup> See generally Louven & Slodczyk, *supra* note 46 (complying with Egypt’s Internet laws appeared to be Vodafone executives only option who feared being arrested by the Egyptian police if they did not comply); see *supra* Part II. A (discussing Vodafone’s compliance with Egypt’s request to shut down the Internet).

<sup>60</sup> See Hope, *supra* note 2, at 19.

<sup>61</sup> In 2010 Google publicly announced that they would cease operating in China if China continued to filter the website. See *Internet Censorship in China*, *supra* note 27. China vehemently supported its Internet policies and declared that any ICT company operating in China would be required to follow the law. *Id.* Google quickly began rerouting its users to Hong Kong’s uncensored Google website. *Id.* After a month long stalemate between the Chinese government and Google, the ICT renewed its operating license with the Chinese government and reactivated it’s website in mainland China in accordance with Chinese Internet laws. *Id.* Google’s acquiescence

## GOOD FOR THE BOTTOM LINE

choose between “moral” responses and refuse to comply with censorship regulations, or choose to ignore the human rights consequences and comply with regulations in order to maintain business operations in that country.<sup>62</sup> Most ICT companies will weigh the success of business over moral concerns and agree to comply with Internet regulations that limit content or disclose user information.<sup>63</sup>

Like many ICT companies, Twitter has recently announced that it will not employ a company policy regarding censorship. Instead, they will censor users’ “tweets” on a country-by-country basis so that it can “keep doing business in countries . . . that do not welcome all [types of] expression.”<sup>64</sup> Additionally, Vodafone’s role during the Egyptian protest in 2011 demonstrates that ICT companies are willing to comply with governments’ demand to censor in lieu of losing business.<sup>65</sup> The reluctance of ICT companies to resist government demands to censor the Internet highlights the need for activists to shape a response to this dilemma that will not only protect the rights of Internet users but also protect the business operations and objectives of ICT companies.

### III. ATTEMPTS MADE BY THE UNITED STATES GOVERNMENT AND THE GNI TO LIMIT ICT COMPLICITY WITH FOREIGN REGIMES WHOSE INTERNET LAWS VIOLATE THE RIGHTS OF EXPRESSION AND PRIVACY

The response of the United States government and private organizations to the Internet censorship crisis has been ongoing. Both public and private entities are attempting to address Internet laws of foreign countries by working to decrease corporate complicity with intrusive foreign government regulations.<sup>66</sup> Advocates appear to be taking a twofold approach in addressing the issues confronted by ICT companies. Private organizations, like the GNI, are working to form an “Internet evolution” where companies choose to self regulate the way in which they assist governments in implementing laws that violate Internet users’ rights.<sup>67</sup> Alternatively, public measures are being taken by the United States government to

---

to Chinese law was seen as its attempt to “keep a foot in China which now has more Internet users than the United States”. *Id.*

<sup>62</sup> See Lynch, *supra* note 25. See also Anjali Bhat, *U.S. Senate Subcommittee Examines American Companies’ Compliance With Censorship Abroad*, SCIENCE AND TECHNOLOGY L. REV. (Mar. 8, 2010), <http://www.stlr.org/2010/03/u-s-senate-subcommittee-examines-american-companies%E2%80%99-compliance-with-censorship-abroad/> (explaining that criminal or civil penalties in the U.S. may simply present U.S. companies with the following calculation: will defying the U.S. law cost them more or less than circumventing internet restrictions in China or Iran? . . . [Companies face] a difficult choice: they must either violate the law at home, or abroad); Clinton, *supra* note 9 (stating that ICT compliance have a “moral” obligation to society and calling on ICT companies to recognize the nexus between morality and economics stating that the moral decision can also reap the financial reward).

<sup>63</sup> See Lynch, *supra* note 25; See also Rajab, *supra* note 8; Louven & Slodczyk, *supra* note 45 (exemplifying ICT compliance during the 2011 protests).

<sup>64</sup> Kevin Dolak & Ned Potter, *Twitter to Censor Tweets Country-by-Country*, ABC NEWS (Jan. 27, 2012), <http://abcnews.go.com/blogs/technology/2012/01/twitter-to-censor-content-on-country-by-country-basis/>.

<sup>65</sup> See Louven & Slodczyk, *supra* note 46.

<sup>66</sup> See Bhat, *supra* note 62; CRS, *supra* note 3, at 16-17.

<sup>67</sup> See Rebecca MacKinnon: *Let’s Take Back the Internet!*, YOUTUBE (Jul. 14, 2011), <http://www.youtube.com/watch?v=PFDoCLf96Kg> [hereinafter MacKinnon, *Take Back the Internet*].

stop ICT companies from complying with unreasonable foreign censorship demands by imposing legal sanctions on ICT companies that uphold oppressive Internet laws.<sup>68</sup>

Scholars and private organizations have shaped their response to ICT complicity with oppressive Internet laws by describing an “Internet evolution” carried out in a “citizen centric manner.”<sup>69</sup> The “citizen centric” approach focuses on all contributors (ICT companies, human rights activist and governments) working together to promote the rights of the Internet user by holding ICT companies accountable for acting contrary to citizen’s best interest.<sup>70</sup>

Rebecca MacKinnon is a leading contributor to the “citizen centric” approach.<sup>71</sup> MacKinnon insists that in order to have Internet innovation, politicians, business advocates and consumers must come together to redefine how the Internet serves users in a quest to be free and less controlled.<sup>72</sup> MacKinnon describes an Internet evolution as a “Magna Carta” moment when citizens and entities around the world demand that governments protect freedom on the Internet and the right to “be connected,” while ICT companies respond uniformly and consistently by protesting the laws that hinder that endeavor.<sup>73</sup>

MacKinnon’s ideology has been adopted by the GNI in an attempt to privately respond to the crisis.<sup>74</sup> Like MacKinnon, the GNI is attempting to create an Internet where “national laws, regulations and policies are consistent with international human rights laws and standards on freedom of expression and privacy.”<sup>75</sup>

The GNI is not the only entity attempting to address ICT compliance with oppressive Internet laws. Public measures, like the Alien Tort Claims Act of 1789 (ATS) and The Global Online Freedom Act are being employed by the United States government to limit ICT complicity with oppressive foreign Internet laws. In 1789, Congress enacted the ATS to convey federal subject matter jurisdiction over “any civil action [brought] by an alien for a tort

---

<sup>68</sup> See Lambrect, *supra* note 7.

<sup>69</sup> See, MacKinnon, *Take Back the Internet*, *supra* note 67.

<sup>70</sup> See *id.* (suggesting that the Internet is the medium between citizens and their governments and since the role of the government is to serve it’s citizens the Internet should be used for the same purpose).

<sup>71</sup> See *id.* MacKinnon proclaims that the preeminent question is based on ensuring that the “Internet evolves in a citizen centric manner.” *Id.*

<sup>72</sup> See *id.* MacKinnon is calling on the ICT market and governments to collaboratively change the way the Internet is being used. See *id.* MacKinnon’s suggests that governments and other private entities must work together to form a solution. See *id.* She does not support a sole government solution because it would delegate to the government the decision regarding what content is protected and what should be limited. See *id.*

<sup>73</sup> See *id.* MacKinnon is comparing internet innovation to the signing of the Magna Carta where Barons of England decided that the “divine right of the king” was not working and they forced King John to sign the Magna Carta, recognizing that even the king had to abide by a “basic set of rules”. *Id.* The signing of the Magna Carta inspired political innovation, which lead to “consent of the governed”. *Id.* “Consent of the governed” is exemplified by the American governance structure where there is no divine rule but laws created by a representative non-tyrannical government. See *id.* The quest to achieve a government based on “consent of the governed” has influenced the movement for Internet innovation and the movement to achieve “consent of the networked”. *Id.* Like the signing of the Magna Carta, achieving “consent of the networked” will require innovation that goes beyond government demands on how the Internet is to be used. See *id.* According to MacKinnon this movement requires “innovation that’s not only focuses on political and and geo political [concerns], but it is also need[s] to deal with questions of business management, investor behavior, consumer choice and even software design and engineering. Each [entity] has a vital part to play in creating a world where government and technology serves the worlds people and not the other way around”. *Id.*

<sup>74</sup> See PRINCIPLES, *supra* note 16 at 1.

<sup>75</sup> *Id.*

GOOD FOR THE BOTTOM LINE

only, committed in violation of the law of nations or a treaty of the United States.”<sup>76</sup> Theoretically, ICT companies could violate the ATS by providing a foreign government with a user’s personal information, which then leads to a tort being committed against that user. While it can be used to impose liability on individuals and nation states, it is unclear whether corporate entities like ICT companies can be held liable for actions contemplated the ATS.<sup>77</sup>

The Second Circuit has recently held that corporations cannot be held directly liable under the ATS because they are not considered individuals as defined by customary international laws.<sup>78</sup> Notwithstanding the Second Circuit’s holding on direct liability, the ATS has been used to hold ICT companies accountable for “aiding and abetting” human rights violations committed by foreign governments.<sup>79</sup> “Offenses [committed by ICT companies] only violate the [ATS] when committed *by or with a state*” . . . [and are] not actionable in U.S. courts . . . if carried out entirely by ICT’s without state involvement.”<sup>80</sup> ICT’s face the risk of assessorial liability when they “provide state authorities with user-identifying information, with knowledge that the state intends to use the information to commit human rights violations.”<sup>81</sup>

Without a definitive answer regarding direct corporate liability under The ATS the Act remains limited in its ability to control ICT companies that are complicit in censoring the Internet.<sup>82</sup> Moreover, the Act has been ineffective in preemptively restricting acts of ICT companies from censoring the Internet, as evidenced by the number of ICT companies expanding into countries where the government limits the use of Internet.<sup>83</sup> Even if ICT companies comply with oppressive foreign Internet laws they will not be in contravention of the Act unless a tort has been committed against the user.

Inconsistencies in the Act’s application may arise because the drafters of the ATS did not contemplate the breadth of the Internet when the ATS was enacted.<sup>84</sup> The perpetually evolving Internet requires a more current law attuned to the ever-changing nature of Internet technology.<sup>85</sup> Complications in the law’s application make it unlikely that the ATS will serve as a deterrent to ICT companies when asked to uphold Internet laws that violate users’ rights of expression and privacy.<sup>86</sup>

Another public measure is the Global Online Freedom Act (GOFA). GOFA is a piece of proposed legislation drafted to “stop the vicious merry-go-round [the United States

---

<sup>76</sup> See Alien Tort Claims Act, 28 USCA § 1350 (1789).

<sup>77</sup> See Bauml, *supra* note 11, at 710-11.

<sup>78</sup> See *Kiobel v. Royal Dutch Petroleum Co.*, 621 F.3d 111 at 149 (2d Cir. 2010) *cert. granted*, 132 S. Ct. 472 (Oct. 17, 2011) (No. 10-1491) (holding that the ATS does not provide subject matter jurisdiction over claims against corporations).

<sup>79</sup> See Brian R. Israel, *Make Money Without Doing Evils? Caught Between Authoritarian Regulations In Emerging Markets and A Global Law of Human Rights, U.S. ICTS Face A Twofold Quandary*, 24 BERKELEY TECH. L.J. 617, 629-630 (2009).

<sup>80</sup> *Id.* (emphasis added).

<sup>81</sup> *Id.* at 636.

<sup>82</sup> See *Lawyers and legislators*, *supra* note 10.

<sup>83</sup> See *id.* Despite confusion over who may be held liable under the ACT, companies fear the breadth of the ATS. See *id.* In 2007, Yahoo! settled with Chinese activist whose information they had provided to the Chinese government amidst the fear of being held liable under ATS. See *id.*

<sup>84</sup> See *id.* (noting that “clearer legislation would help” to resolve some of the issues in applying the ATS against ICT companies).

<sup>85</sup> See *id.*

<sup>86</sup> See *id.*

is] now on of exporting Internet-restricting technologies [to repressive regimes].”<sup>87</sup> Although GOFA was first submitted to Congress in 2006 and has been redrafted several times it has yet to become law.<sup>88</sup> Unlike the ATS, GOFA is a direct attempt by Congress to address the effects of ICT complicity in violating the right to freedom and privacy on the Internet.<sup>89</sup>

GOFA proposes to outlaw the role ICT companies have been permitted to play in assisting governments to censor the Internet.<sup>90</sup> U.S. Rep. Christopher H. Smith (R-NJ), who authored the bill, advocates for legislation, noting that “more democratic activist[s] [are] being arrested through the use of a growing array of Internet censorship and surveillance tools.”<sup>91</sup> Congressman Smith has described the transformation of the Internet from a “freedom plaza” to a “dictators best friend” and believes that GOFA can regulate the role ICT companies have been permitted to play in that transformation.<sup>92</sup>

As drafted, GOFA prohibits ICT companies from exporting technology that may be used to restrict freedom on the Internet.<sup>93</sup> GOFA would also require domestic and international companies who trade on United States’ stock exchanges to disclose the measures they have taken to protect freedom on the Internet when operating abroad.<sup>94</sup> GOFA would impose both civil and criminal liability on companies for non-compliance.<sup>95</sup>

GOFA has faced heavy criticism both domestically and internationally, delaying its enactment. Domestic companies have resisted support for GOFA because the Act’s penalties would force them to either comply with the law or not conduct business in certain countries, thus foregoing potential profit.<sup>96</sup> The inability to conduct business in Internet repressive countries has widespread ramifications impacting international commerce.<sup>97</sup> For example, the strain GOFA will place on international commerce between the United States and China will inevitably force the United States government to choose between supporting the Act or respecting the differences between American and Chinese Internet laws.<sup>98</sup>

---

<sup>87</sup> Press Release, United States Commission on Security and Cooperation in Europe, Chairman Smith Introduces New Global Online Freedom Act (Dec. 9, 2011) *available at* [http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewDetail&ContentRecord\\_id=1043&ContentRecordType=P&ContentType=P&CFID=71574881&CFTOKEN=51978649](http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewDetail&ContentRecord_id=1043&ContentRecordType=P&ContentType=P&CFID=71574881&CFTOKEN=51978649) [hereinafter Press Release Smith].

<sup>88</sup> *See id.*; *See Lawyers and legislators, supra* note 10.

<sup>89</sup> *See Bauml, supra* note 11, at 713.

<sup>90</sup> *See* Press Release Smith, *supra* note 87; *See also* the Global Online Freedom Act of 2011, HR 3605, 112th Cong. § 301(a)(t)(2) (2011).

<sup>91</sup> Press Release Smith, *supra* note 87.

<sup>92</sup> *See id.* If passed GOFA would not only apply to U.S. companies but to the increasing number of foreign IT companies that “raise capital on [U.S.] stock exchanges, including a large number of Chinese Internet companies.” *Id.*

<sup>93</sup> *See* H.R. 3605 § 301(a)(t)(2) (“The Secretary shall prohibit the export of goods or technology on the list established . . . to a government end user in any Internet-restricting country.”).

<sup>94</sup> *See* Press Release Smith, *supra* note 87.

<sup>95</sup> *See* Bhat, *supra* note 62 (“[According to *The Guardian*, the GOFA] would make it illegal for a U.S. company to provide information or technology aiding restriction of internet services.”).

<sup>96</sup> *See id.*

<sup>97</sup> *See* Bauml, *supra* note 11, at 716.

<sup>98</sup> *See id.* at 716-17 (discussing the economic relationship between the U.S. and China noting “Obama’s visit to China reflected a general understanding that the United States’ relationship with China is too vital to jeopardize by passing legislation that has the great potential to upset an already strained situation”).

# GOOD FOR THE BOTTOM LINE

GOFA has been criticized internationally for “seek[ing] to regulate the web activities of foreign countries and businesses by imposing its own [U.S.] unilateral standards.”<sup>99</sup> International criticisms highlight the jurisdictional concerns being raised in light of GOFA.<sup>100</sup> Pursuant to GOFA, the United States government could monitor, regulate and prosecute corporate acts that occur outside the country, even if those acts are in compliance with the laws of the country the ICT company operates in.<sup>101</sup> GOFA’s transnational qualities have lead those who oppose the law to question the United State’s respect for comity between nations and relegates the act to a true unilateral approach at limiting ICT complicity in Internet censorship.<sup>102</sup>

While the attempts made by the United States government and the GNI have not succeeded in curtailing the acts of ICT companies abroad, the GNI may have the greatest chance at success.<sup>103</sup> Unlike GOFA and the ATS, the GNI’s private approach is superior because it proposes a global solution developed through the collaboration of the ICT community, scholars and private and public advocates.<sup>104</sup> The collaborative nature of the GNI allows those involved in the market to shape the policies that will guide their actions abroad, which should increase the likelihood that companies will commit to the policies.<sup>105</sup> Despite its potential to change the manner in which ICT companies operate abroad, the GNI must address its critics and restructure fundamental aspects of the organization to gain momentum and to be effective.<sup>106</sup>

## IV. THE GLOBAL NETWORK INITIATIVE APPLIES BROAD PRINCIPLES AND PROVIDES A FRAMEWORK FOR ICT COMPANIES TO IMPLEMENT WHEN ASKED TO COMPLY WITH INTERNET LAWS THAT VIOLATE THE RIGHT TO EXPRESSION AND PRIVACY ON THE INTERNET

The GNI was launched in 2008 by a group of ICT companies, scholars and private investors with the goal of protecting human rights and the freedom of expression and privacy on the Internet.<sup>107</sup> The founding member companies are Google, Microsoft and Yahoo!.<sup>108</sup> The Principles of the GNI are predicated on the values set forth in the Universal Declaration of Human Rights which protects “the right to freedom of opinion and expression; include[ing]

---

<sup>99</sup> *Russia slams US Global Online Freedom Act as ‘Cold War scheme’*, TV-Novosti, (Dec. 9, 2011, 23:31), <http://rt.com/news/usa-online-freedom-business-181/> (Russ.).

<sup>100</sup> See Bauml, *supra* note 11, at 713.

<sup>101</sup> See *id.*

<sup>102</sup> See *id.* at 716 (noting that GOFA creates a potential for “bad blood” between the U.S. and other revenue sharing countries). GOFA infringes on the comity between nations. See *id.* Comity is the “recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens.” See *id.*

<sup>103</sup> See *id.* at 719.

<sup>104</sup> See Susan Morgan, Exec. Dir., Global Network Initiative, Address at Carnegie Council: Yahoo! and YouTube: Balancing Human Rights and Business (Oct. 5, 2011) (transcript available at <http://www.policyinnovations.org/ideas/video/data/000381>).

<sup>105</sup> See *Lawyers and legislators*, *supra* note 10.

<sup>106</sup> See Downes, *supra* note 19.

<sup>107</sup> See ANNIVERSARY NEWSLETTER, *supra* note 14, at 1.

<sup>108</sup> *Id.*

freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media.”<sup>109</sup>

The structure of the GNI is described in its “foundational documents,” which detail the organizations principles and policies for members.<sup>110</sup> These “foundational documents” are: (1) the GNI Principles on Freedom of Expression and Privacy (Principles), (2) the GNI implementation Guidelines (Guidelines) and (3) the GNI Governance, Accountability & Learning Framework (Framework).<sup>111</sup> Together, these three documents are intended to serve as guidance for member organizations confronted with Internet regulations that fall below the international standard for human rights.<sup>112</sup> The functions served by these documents are described below and because they are intended to work in conjunction with one another they are addressed in ascending order.

### A. The Principles of Freedom of Expression and Privacy

The Principles operate on the premise that ICT member companies should use their unique position in the information and technology (IT) market to advance the spread of knowledge among Internet users.<sup>113</sup> The Principles are intended to establish a broad structure for member companies to follow when operating abroad.<sup>114</sup> This structure provides recommendations to the ICT community on how to protect Internet users’ rights when confronted with Internet regulations and policies that fall short of respecting the rights of expression and privacy.<sup>115</sup>

The Principles were purposefully drafted broadly.<sup>116</sup> Susan Morgan, Executive Director of the GNI explained that “the Principles cover very broad things [so companies] can operationalize [the Principles] into the way in which they do business, thinking through the implications around freedom of expression and privacy.”<sup>117</sup>

---

<sup>109</sup> The Universal Declaration of Human Rights, G.A. Res 60. 217 (III) A, U.N. Doc A/Res/ 217(III) (Dec. 10, 1948). The Declaration of Human Rights defines the freedom of expression as “the right to freedom of opinion and expression; includ[ing] freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” *Id.* Pursuant to the Declaration of Human Rights, the right to privacy means that “[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondences, nor to attacks upon his honour and reputation.” *Id.* In addition to the Declaration of Human Rights, the GNI Principles are predicated on the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights. *See* ANNIVERSARY NEWSLETTER, *supra* note 14.

<sup>110</sup> *See* ANNIVERSARY NEWSLETTER, *supra* note 14, at 1.

<sup>111</sup> *See id.*

<sup>112</sup> PRINCIPLES, *supra* note 16, at 1.

<sup>113</sup> *See id.* The Principles call on ICT companies to ensure “that national laws, regulations and policies are consistent with international human rights laws and standards on freedom of expression and privacy.” *Id.* The Principles are universal but allow ICT companies to adopt them in a manner appropriate for the specific company. *See also* Press Release, Durbin, Coburn to Press Tech Companies on Human Rights Code of Conduct (Aug. 7, 2009) (on file with author), <http://durbin.senate.gov/public/index.cfm/pressreleases?ID=47879b56-3081-4adb-85f7-77ae8ee0bec2> [hereinafter Press Release Durbin] (“[The Principles are] intended to be adaptable to the particular circumstances of companies from all sectors of the ICT industry. . .”).

<sup>114</sup> PRINCIPLES, *supra* note 16, at 1.

<sup>115</sup> *See* Morgan, *supra* note 104.

<sup>116</sup> *Id.*

<sup>117</sup> *Id.*

## GOOD FOR THE BOTTOM LINE

In order for an ICT company to be in accordance with the Principles it must avoid or minimize the impact government regulations have on a user's rights.<sup>118</sup> Members must also take certain measures to protect the personal information of Internet users when confronted with government demands for disclosure.<sup>119</sup>

The Principles primarily serve as a commitment of member companies to incorporate the Principles in corporate actions.<sup>120</sup> While the Principles set forth the goals of the GNI they must be implemented in conjunction with the GNI's Guidelines and Framework.<sup>121</sup> The Guidelines provide companies with direction on how the Principles should be incorporated into corporate activities and the Framework describes how companies are held responsible for implementing the Principles into corporate actions.<sup>122</sup>

### B. Implementation Guidelines

The GNI's Guidelines articulate how member companies can comply with the Principles and provides examples on how to adopt the Principles internally.<sup>123</sup> For example, the Guidelines suggest that companies ask governments to document in writing requests to limit the Internet and not concede to oral demands made by foreign regimes.<sup>124</sup> The Guidelines also require member companies to document instances where its corporate actions may compromise or improve the rights of Internet users.<sup>125</sup>

The Guidelines require that member companies document certain corporate activities via Human Rights Impact Assessments (Assessments).<sup>126</sup> Assessments are used to document circumstances when an Internet user's freedom of expression and privacy are being impacted either negatively or positively as a result of company compliance with government demands. These Assessments are used to develop appropriate risk mitigation strategies that will be adopted within the internal structure of the company.<sup>127</sup> Once documented, member companies should be cognizant of the identified risk when entering new markets, designing new technology and entering into corporate relationships.<sup>128</sup>

---

<sup>118</sup> See, PRINCIPLES, *supra* note 16, at 2. Pursuant to the Principles ICT companies should recognize that the right to freedom of expression and privacy on the Internet should not be restricted, "except in narrowly defined circumstances". *Id.* If an ICT company is forced to remove content or disclose information its actions should always be consistent with internationally recognized laws or standards. See *id.* The GNI calls on ICT companies to ensure that measures taken to comply with foreign Internet laws are proportionate with the need to limit or monitor the Internet. See *id.*

<sup>119</sup> See *id.* at 2.

<sup>120</sup> See *id.* at 3 (recommending that "[p]articipating companies identify circumstances where freedom of expression and privacy may be jeopardized or advanced and integrate these Principles into their decision making in these circumstances."); The GNI recommends that ICT companies "implement the Principles wherever they have operational control. . . . [and] [w]hen they do not have operational control, use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow the Principles." *Id.*

<sup>121</sup> See ANNIVERSARY NEWSLETTER, *supra* note 14, at 1

<sup>122</sup> See *id.*

<sup>123</sup> See GLOBAL NETWORK INITIATIVE, IMPLEMENTATION GUIDELINES 1(2008), available at [https://www.globalnetworkinitiative.org/cms/uploads/1/GNI\\_-\\_Implementation\\_Guidelines\\_1\\_.pdf](https://www.globalnetworkinitiative.org/cms/uploads/1/GNI_-_Implementation_Guidelines_1_.pdf).

<sup>124</sup> See *id.* at 4-5.

<sup>125</sup> See *id.* at 2-3.

<sup>126</sup> See *id.*

<sup>127</sup> See *id.* at 2.

<sup>128</sup> See *id.*



## THE JOURNAL OF INTERNATIONAL BUSINESS &amp; LAW

The Guidelines also require participating companies to develop internal structures to ensure the Principles are incorporated into all levels of company operation.<sup>129</sup> Companies are encouraged to implement the Principles internally by creating a “human rights team” that will ensure that the Principles are incorporated into company “analysis, decision making and [company] operations.”<sup>130</sup> The team should establish written policies and procedures that ensure the protection of user rights and are consistent with the Principles.<sup>131</sup> The team should communicate the Principles to all employees, provide training to employees that are most likely to offend the Principles, and provide “whistle-blowing mechanisms” for employees who wish to confidentially report violations of the standards set forth in the Principles.<sup>132</sup>

Further, the Guidelines require ICT companies to take specific steps when governments restrict user communication or remove content from the Internet. Pursuant to the Guidelines companies should “[i]nterpret government restrictions and demands so as to minimize the negative effect on freedom of expression” and “engag[e] proactively with governments to reach a shared understanding of how restrictions can be applied in a manner consistent with the Principles.”<sup>133</sup>

The Guidelines require companies to act with transparency when restricting or removing content from the Internet and inform users of company policies to disclose personal information.<sup>134</sup> The company must also make users aware of generally applicable local laws and policies that require the company to act in accordance with the government demands to limit content or disclose personal information.<sup>135</sup> This information can be provided to the user through a user agreement contract.

Further, the Guidelines require member companies to provide users with notice when access to content has been removed or when personal information has been requested.<sup>136</sup> Notice will not only provide users with information regarding the laws that require the company to disclose or restrict information but may also alert the user to company policies that are often overlooked in user agreements.

The Guidelines encourage ICT companies to hold governments accountable by asking them to be “specific, transparent and consistent in their demands” to restrict information on the Internet and provide a user’s personal information to the government.<sup>137</sup> By insisting

---

<sup>129</sup> See *id.* at 3.

<sup>130</sup> See *id.*

<sup>131</sup> See *id.* at 3-4.

<sup>132</sup> See *id.* at 4.

<sup>133</sup> *Id.* at 4-5. The Guidelines suggest that member companies “[r]equest clear written communications from the government that explain[s] the legal basis for government restrictions to freedom of expression, including the name of the requesting government entity and the name, title and signature of the authorized official.” *Id.* at 5. The participating company should also “[a]dopt policies and procedures to address how the company will respond in instances when governments fail to provide a written directive or adhere to domestic legal procedure.” *Id.* Member companies can “[c]hallenge the government in domestic courts or seek the assistance of relevant government authorities, international human rights bodies or non-governmental organizations when faced with a government restriction that appears inconsistent with . . . international human rights laws and standards on freedom of expression.” *Id.*

<sup>134</sup> See *id.* at 5.

<sup>135</sup> See *id.* at 6-7.

<sup>136</sup> See *id.* at 6. Companies should “[g]ive. . .notice to users when. . .content has been removed or blocked by the participating company. . .due to government restrictions.” *Id.* Additionally, “[n]otice should include the reason for the action and state on whose authority the action was taken.” *Id.*

<sup>137</sup> See *id.* at 6.

## GOOD FOR THE BOTTOM LINE

that governments are consistent in their demands, companies will be able to draft policies and procedures more uniformly. Consistency and specificity is important because it will help ICT companies convey accurate information to users regarding the regulations and how they may affect the user. These demands should be “consistent with international laws and standards on privacy” and freedom of expression.<sup>138</sup>

The Guidelines provide companies with specific procedures that, when implemented, can protect the users’ rights and advance freedom of expression and privacy on the Internet.<sup>139</sup> While the Guidelines require specific tasks to be undertaken, such as Human Rights Impact Assessments, they do not insist on a particular method for implementation.<sup>140</sup> A company may adopt the Principles and implement the Guidelines into its operations in a way that is appropriate for the region in which it operates. Companies are assessed on the ability to create a practice based on the Guidelines and according to the Principles.<sup>141</sup> The method of assessment is detailed in the Framework.

### C. Accountability and Learning Framework

The GNI and its directors aim to “assist [members] to implement the Principles in a manner that protects both the rights of their users and the safety of their employees when facing demands from governments that may threaten freedom of expression or privacy.”<sup>142</sup> The Framework outlines how member companies will be judged on its implementation of the Principles into its corporate operations.<sup>143</sup> The GNI’s Governance Charter is a supplement to the Framework and provides additional information on how companies will be assessed.<sup>144</sup>

The assessment process serves two significant functions for the organization. First, it allows the Organization to identify reoccurring challenges and create a forum for members to collaborate and develop appropriate strategies to mitigate the risks faced by Internet users.<sup>145</sup> Second, it allows the organization to hold member companies accountable for upholding the Principles they committed to protect when they joined the GNI.<sup>146</sup>

Evaluations are conducted in annual independent assessments of member companies.<sup>147</sup> Companies are provided two years to develop an internal structure based on the Principles.<sup>148</sup> Over the two years, companies produce an annual report that describes the steps taken to implement the Principles internally.<sup>149</sup> After the expiration of the two years the

---

<sup>138</sup> See *id.*

<sup>139</sup> See *id.* at 1 (explaining that the Guidelines provide member companies with a “set of actions that constitute compliance with The Principles “ and detailed guidance on how to be in compliance).

<sup>140</sup> See *id.*; see also *supra* text accompanying note 113.

<sup>141</sup> See GUIDELINES, *supra* note 123, at 1.

<sup>142</sup> GNI, ACCOUNTABILITY FRAMEWORK, *supra* note 18, at 1.

<sup>143</sup> See *id.* at 2-5.

<sup>144</sup> See GLOBAL NETWORK INITIATIVE, GOVERNANCE CHARTER 1 (2008), available at [http://www.globalnetworkinitiative.org/cms/uploads/1/GNI\\_-\\_Governance\\_Charter.pdf](http://www.globalnetworkinitiative.org/cms/uploads/1/GNI_-_Governance_Charter.pdf) [hereinafter GOVERNANCE CHARTER].

<sup>145</sup> See *id.* at 9-10.

<sup>146</sup> See *id.* at 10.

<sup>147</sup> See ACCOUNTABILITY FRAMEWORK, *supra* note 18, at 3-5. An independent assessor is an individual or group of individuals who demonstrate the independence and competency necessary to assess company implementation of the Principles and other core GNI documents. *Id.* at 2.

<sup>148</sup> See *id.* at 5.

<sup>149</sup> See *id.*

## THE JOURNAL OF INTERNATIONAL BUSINESS &amp; LAW

company will select an independent assessor to conduct an evaluation.<sup>150</sup> The member company must provide the assessor with a detailed report describing the internal structure that implements the Principles.<sup>151</sup> The independent assessors will also have access to all relevant company data that is not confidential or protected as a trade secret.<sup>152</sup>

The assessor will use the data collected to prepare a report that “explain[s] each company’s responses to specific government demands, and evaluat[es] the effectiveness of the company responses individually and overall in implementing the Principles.”<sup>153</sup> The member company will have the opportunity to respond in writing to the assessors report before a final decision is furnished by the Organization.<sup>154</sup> The Organization’s decision along with the report and company’s response will be made available to the public.<sup>155</sup> The process of public disclosure is intended to hold ICTs accountable for their actions.

The information collected by the independent assessors and all reports drafted by the company will also be used to develop an annual report issued by the GNI describing the Organization’s progress.<sup>156</sup> The report will describe any emerging trends in the industry that were identified during the assessment process as well as the challenges faced by the Organization and its members.<sup>157</sup> The reports drafted by the Organization, its members and assessors are made available to the public.<sup>158</sup>

The Organization uses the transparent nature of the reports as a mechanism to hold member companies accountable for upholding the Principles.<sup>159</sup> Transparency is used to enforce compliance with the GNI principles by relying on the public to make their opinions on the reports known, and thus serve as encouragement to companies to change the policies that are criticized by the public.<sup>160</sup>

In addition to annual public reports, GNI member companies must also “provide an annual communication to the public acknowledging their participation in the GNI and summarizing their related activities.”<sup>161</sup> Moreover, specific information on any member company may be provided to the public at any time.<sup>162</sup> This information includes “[t]he names of

---

<sup>150</sup> See GOVERNANCE CHARTER, *supra* note 144, at 7-8.

<sup>151</sup> See *id.* at 9-10.

<sup>152</sup> *Id.*

<sup>153</sup> GNI, ACCOUNTABILITY FRAMEWORK, *supra* note 18, at 4.

<sup>154</sup> See *id.*

<sup>155</sup> See GOVERNANCE CHARTER, *supra* note 144, at 11.

<sup>156</sup> See *id.*

<sup>157</sup> See ACCOUNTABILITY FRAMEWORK, *supra* note 18, at 2.

<sup>158</sup> See *id.* at 4. The first independent assessments were completed in 2012. See *First independent assessments of GNI founding companies*, Global Network Initiative (Mar. 6, 2012), [http://www.globalnetworkinitiative.org/newsandevents/First\\_independent\\_assessments\\_of\\_GNI\\_founding\\_companies\\_completed.php](http://www.globalnetworkinitiative.org/newsandevents/First_independent_assessments_of_GNI_founding_companies_completed.php). The GNI noted that “[t]he companies found the use of independent assessors a useful learning process in refining their policies and procedures.” *Id.*

<sup>159</sup> See GOVERNANCE CHARTER, *supra* note 144, at 11. The report will inform the public of “[c]ollective lessons learned regarding the Principles and Implementation Guidelines, including the range of effective responses to threats to freedom of expression and privacy, [i]nformation required to improve the understanding of threats to freedom of expression and privacy across different sectors, geographies, legal systems, and cultural traditions, [and] [f]or each participating company, the GNI Board’s compliant or non-compliant assessment.” *Id.*

<sup>160</sup> See *id.*

<sup>161</sup> *Id.*

<sup>162</sup> See *id.* at 12.

participating companies, NGOs, investors, or academic institutions, [w]hether a participant is in good standing as a member of the GNI, [and] [a] summary of the actions taken by a participant to promote the [GNI] Principles. . . .”<sup>163</sup>

The GNI’s Framework is a unique solution to the censorship crisis because it allows companies to direct the manner in which they uphold the Principles and honors a company’s choice to continue operating in a country with strict Internet policies.<sup>164</sup> Together, the three core GNI documents are meant to serve as a commitment of the member companies to protect freedom of expression and privacy on the Internet.<sup>165</sup> The Principles exemplify the commitment to respect users’ rights when faced with strict government regulations limiting content or disclosing user information.<sup>166</sup> The Guidelines provide detailed advice to ICT companies on how to integrate the Principles internally. Lastly, the implementation of the Principles is judged through assessments outlined in the Framework.<sup>167</sup>

## V. THE GNI MUST ATTRACT MORE PARTICIPANTS AND GARNER THE SUPPORT OF THE UNITED STATES GOVERNMENT TO BE SUCCESSFUL IN LIMITING ICT COMPLICITY WITH FOREIGN INTERNET LAWS THAT VIOLATE THE RIGHTS OF EXPRESSION AND PRIVACY

Proponents of the GNI were optimistic early on and praised the GNI for creating a structure that ICT companies could follow when working in countries that censored the Internet.<sup>168</sup> However, four years after its formation the GNI has not reached the level of success predicted. Few ICT companies aside from its founding members have joined the GNI, thus preventing the Organization from upholding their own Principles.<sup>169</sup>

While public and private figures have commended the goals of the GNI, criticisms of the Organization have been predicated on its inability to convince other ICT companies to join.<sup>170</sup> Its failure to recruit members has been blamed on the GNI’s complex governance structure and a fear of a rigorous assessment process, both of which require companies to dedicate corporate funding and employee time to be in compliance with the Principles.<sup>171</sup>

<sup>163</sup> *Id.*

<sup>164</sup> See PRINCIPLES, *supra* note 16, at 5 n. 13 (“Recognize[ing] that participants may take different positions on specific public policy proposals or strategies, so long as they are consistent with the Principles”). See Kopytoff, *supra* note 22 (noting that the “code offers flexibility.”).

<sup>165</sup> See *Core Commitments*, GLOBAL NETWORK INITIATIVE (2008), <http://www.globalnetworkinitiative.org/corecommitments/index.php>; see also Rebecca MacKinnon, *Is the Global Network Initiative Making a Difference?*, RCONVERSATION (May 31, 2009), <http://rconversation.blogs.com/rconversation/2009/06/is-the-global-network-initiative-making-a-difference.html> [hereinafter Mackinnon, *Is the Global Network Initiative Making a Difference*] (“Joining GNI is a public commitment to users that you’re not just going to talk the talk, but you’re going to walk the walk in a transparent, accountable, and credible way.”).

<sup>166</sup> See CORE COMMITMENTS, *supra* note 164.

<sup>167</sup> See *id.*

<sup>168</sup> See Israel, *supra* note 79, at 651 (Commending the GNI a year after its establishment for being a “positive step towards alleviating the business quandary” experienced by ICT companies when asked by a foreign country to censor the Internet).

<sup>169</sup> See Jackie Cohen, *U.S. Senator Asks Facebook For Anonymity Option*, *Mediabistro* (Feb. 11th, 2011, 3:28pm), at <http://www.allfacebook.com/u-s-senator-asks-facebook-for-anonymity-option-2011-02> (quoting Sen. Richard Durbin’s [D-IL], “the GNI has great potential to advance human rights if members companies fully implement the GNI’s Principles and membership is expanded”).

<sup>170</sup> See Kopytoff, *supra* note 22.

<sup>171</sup> See *id.*; Downes, *supra* note 19.

Furthermore, the GNI has incurred criticism for not attracting important members such as Facebook and Twitter.<sup>172</sup> Government officials have pleaded with Facebook (on behalf of the GNI) to no avail.<sup>173</sup> Facebook refuses to join, providing a litany of reasons why its membership to the GNI is unnecessary. Its reasons include the lack of physical offices in many of the countries targeted by the GNI and the ability of Facebook to create its own policies regarding censorship and the protection of personal information.<sup>174</sup> It has also been suggested that ICT companies are concerned with the GNI's aim to make company operations transparent, thus creating negative public exposure for ICT companies.<sup>175</sup>

It is important that companies like Facebook and Twitter join the GNI as they become increasingly more active in the global community. While Google allows users to search the Internet, Facebook and Twitter allow users to complain about oppressive regimes, organize protests and interact with other Internet users globally.<sup>176</sup> Facebook and Twitter played a crucial role in the 2011 political uprisings in Egypt by allowing users to post information and pictures that portrayed the violence against protestors at the hands of Egyptian officials.<sup>177</sup> Most notably, Egypt's order that Facebook and Twitter be shut down during the protest exemplifies how important social media companies are. Without them, it will be increasingly difficult for those who do not agree with their countries laws to protest for change.

If the GNI does not attract more members it will become a fruitless effort.<sup>178</sup> Because the ICT community is so large, there needs to be a majority of companies that agree to comply with the GNI's Principles. If the GNI does not expand the companies that have agreed to uphold its Principles will be replaced by "less scrupulous" ICT companies that are willing to conform to strict Internet laws.<sup>179</sup> The Organization cannot exist with the commitment of only a few companies, no matter how large and powerful those companies are.<sup>180</sup>

---

<sup>172</sup> See Kopytoff, *supra* note 22.

<sup>173</sup> See Lambrect, *supra* note 7.

<sup>174</sup> See Cohen, *supra* note 169.

<sup>175</sup> See *id.*

<sup>176</sup> See CRS, *supra* note 3, at 1. It was additionally noted that "blogs, e-mails, social networks, and text messages are opening up a new virtual town square where citizens can go to criticize their governments and exchange ideas." *Id.* at 14.

<sup>177</sup> See Alexander, *supra* note 50; Galperin, *supra* note 45. See also John Moe, *Global Network Initiative is Withering on the Vine*, AMERICAN PUBLIC MEDIA (Mar. 7, 2011, 8:00 a.m.) <http://www.publicradio.org/columns/marketplace/tech-report/2011/03/global-network-initiative-is-withering-on-the-vine.html> ("This matters - a lot - because when the internet is really being used as a tool against oppressive regimes, THOSE are the companies that are being employed") (emphasis in original).

<sup>178</sup> See Kopytoff, *supra* note 22.

<sup>179</sup> See Brendan Ballou, *Global Online Freedom Act: Governments Can't Protect Freedom by Themselves*, THE FUTURE OF THE INTERNET (Jul. 18th, 2008), <http://futureoftheinternet.org/global-online-freedom-act-governments-cant-protect-freedom-by-themselves> (explaining that when U.S. companies don't uphold the laws of a foreign country "less scrupulous foreign companies . . . take their place"); MacKinnon, *Is the Global Network Initiative making a difference?*, *supra* note 164. The GNI has also failed to gain the support of foreign companies who view the Initiative as a purely "Western" organization. See *id.* The inability to attract other companies is a problem for the GNI because many of those companies will simply take over the business of GNI members seeking to protect the rights of Internet users in foreign countries. See Lynch, *supra* note 25 (explaining that if companies reject demands to censor the Internet they will be put out of business and replaced by other companies willing to censor).

<sup>180</sup> See Kopytoff, *supra* note 22.

GOOD FOR THE BOTTOM LINE

It is clear that economics play a large role in a company's decision to join the GNI. This issue is highlighted in the relationship between U.S. companies and China.<sup>181</sup> ICT companies depend on China (which boasts the world's largest internet using population) for economic revenue and thus ICT companies do not want to jeopardize their standing with the Chinese government.<sup>182</sup> If the ability to conduct business in China is compromised, the company's revenue will decrease; thus ICT companies often comply with governments like China, valuing economic gain over the user's rights.<sup>183</sup>

Both Chinese activists and U.S. scholars have referenced the lack of economic benefit associated with upholding the GNI Principles in foreign countries that censor the Internet.<sup>184</sup> Although the GNI does not require companies to reject a government's Internet policy, it will nonetheless risk a loss in revenue when upholding the GNI's Principles abroad.<sup>185</sup> For example, the GNI requires companies to demand written requests from governments seeking to limit or disclose information.<sup>186</sup> While a government can easily acquiesce and provide a written demand, the request could also be refused and transpire into an expensive and time-consuming dispute. While large ICT companies like Google have the funding to implement ICT Principles internally and expense time-consuming disputes, small startup companies do not have the same financial security to dedicate to upholding the Principles.<sup>187</sup>

Though frustration regarding the success of the GNI is mounting in the private and public arena, it is the preeminent option compared to the solutions set forth by the government.<sup>188</sup> Government representatives are being forced to weigh the value of their relationships with many countries before asserting its position on Internet censorship.<sup>189</sup> Legislative means appear to be withering in the face of jurisdictional issues, meager support among companies most affected by the legislation, and failure to consider the international standard of comity among nations.<sup>190</sup> While the GNI has faced criticism, the issues engendered in a private remedy appear minimal in the face of failed public action.

Government support of the GNI has varied since the organization was established in 2008.<sup>191</sup> Government support, once steeped in commendation, has since evolved into threats

---

<sup>181</sup> See Bauml, *supra* note 11, at 716.

<sup>182</sup> See *id.* at 716. Bauml suggests that it may be more beneficial to allow ICT companies to stay in China rather than create legislative restrictions that prohibit business in China and other Internet-censoring countries, especially considering that China holds roughly \$800 billion of U.S. debt and the Chinese economy is dependent on U.S. goods - like those produced by ICT companies. See *id.* at 729, 732.

<sup>183</sup> See Lynch, *supra* note 25 (explaining that if ICT companies do not comply with Chinese law they will "put out of business" and replaced by companies that will comply with Internet laws).

<sup>184</sup> See Lin Xiaofan, *The Colour of Money vs. Human Rights Values*, EPOCHWEEKLY (Mar. 7 2008) <http://epochweekly.com/b5/099/5605.htm>.

<sup>185</sup> See Downes, *supra* note 19.

<sup>186</sup> See GUIDELINES, *supra* note 123 at 5.

<sup>187</sup> See Downes, *supra* note 19; See also Zhen, *supra* note 8 (explaining that it is easier for the GNI to encourage members to uphold GNI principals in places like Libya or North Korea because there is "no economic benefit" and it difficult to uphold the GNI's principals in China because there is a large economic interest).

<sup>188</sup> See Bauml, *supra* note 11, at 719.

<sup>189</sup> See *id.* At 716-17.

<sup>190</sup> See *id.* at 717; *supra* text accompanying note 102.

<sup>191</sup> See Downes, *supra* note 19.

## THE JOURNAL OF INTERNATIONAL BUSINESS &amp; LAW

of legislation aimed at companies that do not support the private movement.<sup>192</sup> Sen. Richard Durbin [D-IL] has manned the crusade against companies that failed to join the GNI.<sup>193</sup> Rallying behind the GNI early on, Sen. Durbin stated in a 2009 letter to ICT companies, “the [GNI] has great potential to advance and protect human rights if member companies fully implement the GNI’s Principles and the GNI’s membership is expanded.”<sup>194</sup>

The hope that companies would engage in the GNI’s mode of self-regulation quickly transpired into frustration with those who did not join the organization.<sup>195</sup> Excuses proffered by companies like Facebook and Twitter appeared futile in the face of the censorship epidemic.<sup>196</sup> Congressional representatives have refused to accept excuses such as “[Facebook does not plan to join] unless and until the growth [of its] international business warrants it and [it] ha[s] the staff hours to dedicate to the initiative.”<sup>197</sup>

The refusal by Facebook and Twitter to take part in a 2010 hearing conducted by Sen. Durbin on the issue of human rights and the Internet was the ultimate insult.<sup>198</sup> Sen. Durbin retaliated against the companies who refused to join the GNI by threatening to take legislative action stating, “[if] U.S. companies are unwilling to take reasonable steps to protect Human rights, Congress must step in.”<sup>199</sup> Sen. Durbin’s mounting frustration was evident as he explained the need for legislative action “when major multimillion-dollar and multibillion-dollar companies will not even join the conversation about human rights. . . .”<sup>200</sup> Strong-armed comments have not resulted in increased company enrollment and may be hazardous to the growth of the GNI as ICT companies do not appear to be easily intimidated into participation.

Since 2010 congressional representatives have rallied behind federal legislation that will ultimately bring criminal penalties against companies that comply with foreign demands to censor the Internet.<sup>201</sup> While GOFA has been redrafted several times, critical issues in the Act have consistently kept the bill from passing. GOFA’s failure has forced scholars to consider which method is better to address global censorship: unilateral legislation or the “citizen centric” approach proffered by the GNI.<sup>202</sup> Jessica E. Bauml succinctly articulated the differences between the two approaches:

---

<sup>192</sup> See *id.*

<sup>193</sup> See Lambrect, *supra* note 7.

<sup>194</sup> Press Release Durbin, *supra* note 113.

<sup>195</sup> See Downes, *supra* note 19.

<sup>196</sup> See *id.*

<sup>197</sup> Lambrect, *supra* note 7. See also Alfonso Serrano F., *The Social Media Explosion: By the Numbers*, THE FISCAL TIMES (Sep. 12, 2011), <http://www.thefiscaltimes.com/Articles/2011/09/12/The-Social-Media-Explosion-By-the-Numbers.aspx#page1>. In 2011 Twitter had 100 million users worldwide and was valued at \$8 billion; Facebook had 750 million users worldwide and is currently valued at roughly \$800 billion. *Id.* Moreover, Facebook produced revenue over \$1.6 billion in 2011 and its membership is projected to reach 1 billion users worldwide this year. *Id.* Approximately 80% of Facebook users are outside the U.S. and Canada and Facebook currently maintains 3,000 employees. *Fact Sheet*, FACEBOOK (2012), <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22>.

<sup>198</sup> See Lambrect, *supra* note 7.

<sup>199</sup> See *id.*

<sup>200</sup> See *id.*; *supra* text accompanying note 197 (explaining the valuations of Facebook and Twitter).

<sup>201</sup> See Lambrect, *supra* note 7.

<sup>202</sup> See Bauml, *supra* note 11, at 712-21(2011).

GOOD FOR THE BOTTOM LINE

[T]he GNI appears to tackle some of the critical issues inherent in GOFA. The GNI attempts to address on a global scale issues that GOFA sought to address through only the narrow lens of American law. Likewise, the GNI creates a forum for disseminating information on international laws and provides assistance to companies in order to help them minimize their contributions to human rights violations. Most importantly, it places all participating [ICT's] on a level playing field by creating uniform guidelines for every company and enabling these companies to work together to oppose government demands that potentially compromise human rights.<sup>203</sup>

The movement to decrease Internet censorship remains in the crossroads while the GNI's aptitude for success remains uncertain and Congress fails to garner support for federal legislation.<sup>204</sup> Moreover, an unstable economy makes it increasingly likely that Internet censorship will take a back seat in the U.S. agenda, especially when maintaining a positive relationship with countries like China is most important.<sup>205</sup> The method proposed by the GNI may have the greatest chance at success because it assumes a global approach and respects comity between nations.<sup>206</sup> Unlike GOFA and any other legislation drafted by Congress, the GNI is premised on international laws and seeks to engage other corporations, scholars, NGO's and governments who value freedom of privacy and expression on the Internet.

In light of the issues faced by the United States government in battling corporate censorship, Congress should direct its energy to supporting the GNI, as it did when the organization was founded, and develop positive incentives for companies who join. In order for the GNI to survive it must recruit more members and it is imperative that the government work with the GNI in this undertaking.

**VI. THE UNITED STATES GOVERNMENT SHOULD WORK WITH THE GNI AND ITS MEMBERS TO PROVIDE INCENTIVES FOR ICT COMPANIES THAT AGREE TO JOIN THE ORGANIZATION**

While the Principles and Framework set forth by the GNI are more practical than any solution proffered by Congress, it will not succeed unless it garners more support within the ICT community. In order for the GNI to garner more support, both private and public advocates must recruit members and combat Internet censorship primarily through the structure offered by the GNI.<sup>207</sup>

---

<sup>203</sup> Bauml, *supra* note 11, at 719 (discussing the different remedies used to address Internet censorship including GOFA and the GNI but ultimately concluding that each method "fails to address fully the problems that arise from corporate complicity" and postures that the focus should not be on the ICT's but should be directed towards the countries that limit the internet).

<sup>204</sup> See *id.* at 717, 721 (noting that it is unlikely GOFA will pass but also noting that there are issues associated with the GNI that make its potential for success questionable).

<sup>205</sup> See Stephen Kaufman, *Societies Free from Censorship on the Internet are Stronger, Obama Says*, EFL-BURKINA (Nov. 17, 2009), <http://www.elearning-burkina.com/washington-files/386-societies-free-of-internet-censorship-are-stronger-obama-says.html> (discussing remarks made by President Obama regarding the growth in trade between the United States and China).

<sup>206</sup> See Bauml, *supra* note 11, at 720; see also *supra* next accompanying note 102.

<sup>207</sup> See Press Release Durbin, *supra* note 113 (recognizing that the GNI has potential to succeed if it gains more members and attempting to use position as public figures to convince companies to join).



## THE JOURNAL OF INTERNATIONAL BUSINESS &amp; LAW

The United States government must provide the GNI the time and support it needs to succeed by incentivizing membership and suspending its threats of legislation.<sup>208</sup> Government representatives should collaborate with members in the ICT community to establish what measures Congress can take to encourage and incentivize membership.<sup>209</sup> The attempt of Congress to criminalize corporate compliance is pushing ICT companies in the wrong direction and has not been successful in persuading members to join the GNI.<sup>210</sup> Considering the unlikelihood that GOFA will pass, using the legislation as a threat only serves to deter companies from wanting to assist the government to advance freedom on the Internet.<sup>211</sup>

Congress must refocus its energy dedicated to upholding Internet freedom onto the GNI so that the two groups- private companies and the government- can jointly find amenable solutions and incentives to increase membership.<sup>212</sup> The United States State Department currently allocates over \$50 million for a range of programs that support Internet freedom and it could benefit the GNI if a fraction of that funding was dedicated to the Organization.<sup>213</sup> Incentives may include the appropriation of federal funding provided to the GNI for the purpose of recruiting more members.<sup>214</sup> Federal funding may also be offered to ICT companies in exchange for its commitment to join the GNI and uphold the Principles.<sup>215</sup> The amount of money allocated by the state department should be based on the calculated cost incurred by ICT companies who join the GNI. This calculation should include, but not be limited to, the cost associated with creating an internal department dedicated to upholding the GNI's Principles and the cost of complying with the GNI's Guidelines when faced with demands to censor the Internet.<sup>216</sup>

---

<sup>208</sup> See Lambrect, *supra* note 7. The "conversations" between Congress and ICT companies were not given enough of a chance as threats of legislation were proffered immediately after ICT companies refused to attend hearings on human rights and the internet. See *id.* Collaboration should be resumed as the conversation was called off too soon and only in retaliation against ICT companies that appeared resistant to joining the GNI.

<sup>209</sup> See Press Release Durbin, *supra* note 113. While previous attempts at working with members of the market have not been successful representatives should reach out to ICT companies again but instead offer an incentive to cooperate.

<sup>210</sup> See *id.* (explaining to ICT companies that if they do not consider joining the GNI "it may be necessary for Congress to consider legislation to ensure that companies take measures [to protect human rights]"). It does not appear that threats of legislation have encouraged ICT companies to join the GNI. See Participants, *supra* note 9. There are currently 31 members of the GNI, but only a fraction of those members are ICT companies. See *id.* These failures highlight the need for a compromise as "[t]he problems with [GOFA] show that the government cannot protect the Internet openness by itself. . . . [S]ome of [the] responsibility for protecting freedom and innovation [should shift] towards interested individuals and responsible [ICT] companies." Ballou, *supra* note 73.

<sup>211</sup> See generally Ballou, *supra* note 73 (discussing the need for the government and private companies to collaborate).

<sup>212</sup> See Clinton, *supra* note 9 (explaining that more needs to be done to limit corporate complicity and that the United States must "work together with the private sector" because there is a shared responsibility between the government and private companies to safeguard freedom on the internet).

<sup>213</sup> CRS, *supra* note 3, at 12.

<sup>214</sup> See CRS, *supra* note 3, at 15 (noting that Secretary of State Clinton has discussed the allocation of \$15 million from the state department "to a range of programs that in, in full or in part, support internet freedom").

<sup>215</sup> See *id.* at 12. Congress has appropriated \$50 million since 2008 to support internet freedom globally. *Id.* at 12. The federal money dedicated to internet freedom is provided by The State Department through "both earmarked and other foreign assistance funding to support Internet freedom, independent media, and the free flow of information." *Id.*

<sup>216</sup> See Downes, *supra* note 19 (explaining the significant costs associated with participating in GNI including the demand for employee time and resources dedicated to incorporating and upholding the Principles).

## GOOD FOR THE BOTTOM LINE

Additionally, it behooves the current members of the GNI to independently incentivize membership.<sup>217</sup> For example, Google and Yahoo! could decrease the cost of website advertisements for smaller ICT companies in return for joining the GNI.<sup>218</sup> Microsoft could also offer some of their products at discounted rates to ICT companies that join the GNI, similar to the discounts they currently offer to small businesses.<sup>219</sup> The amount allocated by the current members of the GNI should be based on the calculated cost incurred by ICT companies who join the GNI and should decrease if federal funding is provided to the Organization.<sup>220</sup>

Current members of the GNI should also use their influential positions in the ICT community to publicly support other ICT companies that join. For instance, Google could issue advertisements each time an ICT company agrees to join the GNI and include a synopsis on the new member. Publicly promoting ICT companies that join the GNI will help to develop consumer trust for the new member as well as bring recognition to the GNI and its founding members.<sup>221</sup>

If the United States government and GNI work together to financially incentivize membership, ICT companies will have fewer reasons to reject requests for participation. For example, Facebook currently finds it imprudent to dedicate employee hours to uphold the GNI's Principles when they do not have physical offices in many of the countries targeted by the GNI.<sup>222</sup> If Facebook is offered financial incentives they may be willing to disregard the lack of physical offices in some countries and use the funding to uphold GNI principles in the countries it currently operates in.

## VII. CONCLUSION

Private ICT companies are continually relied on by foreign governments to censor the Internet.<sup>223</sup> Despite the attempts of private organizations and the United States government acts of ICT complicity have not diminished.<sup>224</sup> While advocates in the public and private arena share the goal of protecting the rights of expression and privacy on the Internet, they have taken opposite positions on how to reach that objective.<sup>225</sup> The United States gov-

---

<sup>217</sup> The motives of the three founding members, Google, Microsoft and Yahoo!, was questioned when the GNI was first established. See Xiafon, *supra* note 184. Critics questioned whether the founding members were truly dedicated to advocate against censorship or whether they wanted to improved public perception of the companies. See *id.* Four years after the GNI's establishment critics still questioned whether the three founding members are dedicated to the GNI. See Downes, *supra* note 19. If the founding companies want to dispel notions of self interest they should dedicate more energy towards promoting the GNI.

<sup>218</sup> See *Paid Search Advertising: Google AdWords, Yahoo Search Marketing & Microsoft adCenter*, SEARCH ENGINE WATCH (Mar. 11, 2011), <http://searchenginewatch.com/article/2064567/Paid-Search-Advertising-Google-AdWords-Yahoo-Search-Marketing-Microsoft-adCenter> (explaining how Google, Yahoo!, and Microsoft allow other companies to advertise on their search engines for a fee).

<sup>219</sup> See Eric Lai, *Microsoft discounts Windows 7 for small businesses*, COMPUTERWORD, (Sep. 1, 2009), [http://www.computerworld.com/s/article/9137383/Microsoft\\_discounts\\_Windows\\_7\\_for\\_small\\_businesses](http://www.computerworld.com/s/article/9137383/Microsoft_discounts_Windows_7_for_small_businesses).

<sup>220</sup> See *supra* text accompanying note 215.

<sup>221</sup> See Clinton, *supra* note 9 (explaining how consumer trust translates into a better and more successful business).

<sup>222</sup> See *supra* part III.

<sup>223</sup> See *supra* Part II. B.; *supra* text accompanying note 54.

<sup>224</sup> See *supra* Part II. A.

<sup>225</sup> See *supra* Part III.

ernment has unsuccessfully sought to limit ICT compliance by imposing criminal and civil penalties against ICT companies when they comply with foreign laws that violate the user's rights of expression and privacy.<sup>226</sup> Alternatively, the GNI has attempted to reform the ICT community by calling on ICT companies to self-regulate acts of compliance and insert social responsibility into corporate activities.<sup>227</sup>

Despite difficulties in recruiting members, the GNI offers the paramount strategy for curbing acts of ICT complicity. The Framework offered by the GNI balances the concerns of ICT companies with the need to monitor and report when governments are using ICT companies to violate a user's rights to freedom of expression and privacy on the Internet.<sup>228</sup> By balancing multiple concerns the GNI has the ability to protect ICT companies' right to conduct business abroad while documenting and shaping an appropriate response to governments' request to censor the Internet.

It benefits all proponents of Internet freedom if the government and current members of the GNI come together to promote the Organization and provide incentives for ICT companies to join. If public and private parties work together to financially entice GNI membership, there is a greater chance that the GNI and its Principles can succeed in protecting and promoting the rights of expression and privacy on the Internet. A substantial rise in corporate participation would significantly increase the GNI's ability to redefine how the Internet is used in a manner that upholds the rights of expression and privacy.

---

<sup>226</sup> *See id.*

<sup>227</sup> *See supra* Part III. A-C.

<sup>228</sup> *See supra*, text accompanying note 113.