

NOTE

“Yes We Scan”: Using SEC Disclosures to Compel and Standardize Tech Companies’ Reports on Government Requests for User Data

Ana M. González*

ABSTRACT

The recent Snowden leaks have ignited fiery debates over government requests for private user information and tech companies’ complicit role in bulk data collection. Some information and communications technology firms have urged government to reform its surveillance practices for private user data. Many others, however, remain silent. This Note argues that Congress should compel Internet and telecommunications companies to make a standardized disclosure when the government requests data. A flexible SEC disclosure for government requests meets the twin aims of satisfying companies’ desire to supply the public with information, while setting a precedent of government accountability for the future. This solution also standardizes the for-

* J.D., expected May 2015, The George Washington University Law School; B.A., Political Science and French and Francophone Studies, 2012, University of Florida. Warmest thanks to the staff of *The George Washington Law Review* for helping make this Note a reality. I would also like to acknowledge Professors Dawn C. Nunziato and John Walker for their advice during the writing process. Finally, I would like to extend my deepest gratitude to my family and friends for their continuing love and support.

Note that “Yes We Scan” is taken from Juliet Lapidus’s *Yes We Can to Yes We Scan*, N.Y. TIMES (July 18, 2013, 3:55 PM) (reporting on slogans that protesters used in reaction to leaks detailing the National Security Agency’s surveillance practices, several of which parodied some of Barack Obama’s “Hope” and “Yes We Can” campaign catchphrases), http://takingnote.blogs.nytimes.com/2013/07/18/yes-we-can-to-yes-we-scan/?_r=0.

mat and substance of transparency reports. Because the few companies that currently publish reports do so in vastly different manners, the proposed disclosure would provide the industry with a much-needed uniform transparency model.

TABLE OF CONTENTS

INTRODUCTION	1059
I. THE NEED FOR DISCLOSURE AND EFFORTS TO ACHIEVE IT	1064
A. <i>The Global Network Initiative: ICT Self-Regulation and the Development of a Government Requests Reporting Standard</i>	1064
B. <i>Failed Legislation: The Global Online Freedom Act</i>	1068
II. A USEFUL FRAMEWORK: THE SEC AND “COMPLY-OR- EXPLAIN” DISCLOSURES	1071
A. <i>The SEC: A Vehicle for Public Disclosure</i>	1072
1. Dodd-Frank’s Extractive Industry Provision: What Not to Do	1072
2. Dodd-Frank’s Conflict Minerals Disclosure: A Lesson in Implementation	1075
B. <i>Comply-Or-Explain: Toward a “Hard Law” Best Practice</i>	1077
1. Definition and Application in the European Corporate Context	1078
2. Sarbanes-Oxley: Comply-or-Explain in the U.S. Corporate Context	1080
III. SEC COMPLY-OR-EXPLAIN DISCLOSURE RULE ON GOVERNMENT REQUESTS FOR USER DATA	1082
A. <i>“ICT Company” Defined</i>	1083
B. <i>Transparency Report: Government Requests Chart in Form and Substance</i>	1084
C. <i>Interpretive Guidance on “Explain”</i>	1087
CONCLUSION	1088
APPENDIX	1089

INTRODUCTION

“The security of users’ data is critical, which is why we’ve invested so much in encryption and fight for transparency around government requests for information. This is undermined by the apparent wholesale collection of data, in secret

and without independent oversight, by many governments around the world. It's time for reform and we urge the US government to lead the way.”¹

—Larry Page, CEO, Google

“Reports about government surveillance have shown there is a real need for greater disclosure and new limits on how governments collect information. The US government should take this opportunity to lead this reform effort and make things right.”²

—Mark Zuckerberg, CEO, Facebook

In 2006, Yahoo faced criticism for aiding and abetting the torture and imprisonment of Chinese journalist Shi Tao.³ Two years earlier, the Beijing State Security Bureau had submitted a request to Yahoo for Tao's user email account, IP address, and activity time logs, citing as its legal basis “[the user's] illegal provision of state secrets to foreign entities.”⁴ The Chinese government subsequently kidnapped Shi Tao, detained him for weeks without charging him with any crime, and finally sentenced him to ten years in prison without trial.⁵ The families of Shi Tao and Wang Xiaoning, another political dissident who faced persecution after Yahoo revealed information to China, sued Yahoo under an aiding and abetting theory.⁶ After being called to Capitol Hill to answer for the allegations, Yahoo was shamed into settling the case with the families of Shi Tao and Wang Xiaoning.⁷

Other tech giants also came under fire in 2006 for bending to Beijing's demands.⁸ In particular, public outcry followed a report that Microsoft had shut down a “well-known” Chinese blogger's site at Beijing's behest “after he discussed a high-profile newspaper strike

1 REFORM GOVERNMENT SURVEILLANCE, <http://reformgovernmentsurveillance.com> (last visited Mar. 17, 2015) [hereinafter *Open Letter to Washington*].

2 *Id.*

3 Brian R. Israel, “*Make Money Without Doing Evil?*” *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, 617–18 (2009); Erick Schonfeld, *Analysis: Yahoo's China Problem*, CNN MONEY (Feb. 8, 2006, 8:23 PM), http://money.cnn.com/2006/02/08/technology/yahoo_china_b20/.

4 Israel, *supra* note 3, at 617 (internal quotation marks omitted) (citing Beijing State Security Bureau, Notice of Evidence Collection, 2004 BJ State Sec. Ev. Coll. No. 02, *original and English available at* http://www.duihua.org/press/news/0730_policedoc.pdf).

5 *Id.*

6 *Id.* at 617–18.

7 *See id.* at 618.

8 David Barboza & Tom Zeller, Jr., *Microsoft Shuts Blog's Site After Complaints by Beijing*, N.Y. TIMES, Jan. 6, 2006, at C3.

that broke out” in Beijing one week earlier.⁹ Google likewise suffered backlash for introducing censored versions of its search engine to comply with the Chinese government’s information filtering requirements.¹⁰

The recent leaks by Edward Snowden, a former IT security employee at the Central Intelligence Agency (“CIA”) and IT security contractor for the National Security Agency (“NSA”), who revealed documents about the reach of the NSA’s web of surveillance in the United States and across the globe, have reignited 2006’s fiery debates over government requests for private user data.¹¹ This time, however, it is the United States government that is attempting to assert influence over tech companies.¹² One of Snowden’s revelations indicated that “the NSA has direct access . . . to the servers of some of the biggest U.S. tech companies, including Apple, Google and Microsoft,”¹³ resulting in access to the emails, stored data, and online social networking details of millions of Americans and individuals abroad.¹⁴ Apparently, these large tech companies helped NSA to “circumvent [users’] encryption and other privacy controls” in return for handling the companies’ costs of compliance.¹⁵ While the tidal wave of Snowden exposés crashed upon the executive branch, customers criticized tech companies for capitulating to egregious government demands for private user data.¹⁶

In Snowden’s aftermath, some information and communications technology firms (“ICTs”)¹⁷ have urged government accountability

⁹ *Id.*

¹⁰ George G. Brenkert, *Google, Human Rights, and Moral Compromise*, 85 J. BUS. ETHICS 453, 454 (2009).

¹¹ See Mark Mazzetti & Michael S. Schmidt, *Ex-C.I.A. Worker Says He Disclosed U.S. Surveillance*, N.Y. TIMES, June 10, 2013, at A1. Snowden fled from Hawaii to Hong Kong and then to Russia after providing these documents to journalists. See Joshua Eaton, *Timeline of Edward Snowden’s Revelations*, AL JAZEERA AMERICA, <http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html> (last visited Mar. 17, 2015).

¹² See Eaton, *supra* note 11 (noting that the United States, through its PRISM program, has access to major companies’ servers); see also Craig Timberg, *U.S. Threatened Massive Fine to Force Yahoo to Release Data*, WASH. POST (Sept. 11, 2014), http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html.

¹³ Eaton, *supra* note 11.

¹⁴ See *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (July 10, 2013), <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>.

¹⁵ Eaton, *supra* note 11.

¹⁶ See Nicole Perlroth & Vindu Goel, *Internet Firms Step Up Efforts to Stop Spying*, N.Y. TIMES, Dec. 5, 2013, at A1; Edward Wyatt & Claire Cain Miller, *Tech Giants Call for Surveillance Curbs*, N.Y. TIMES, Dec. 9, 2013, at B1.

¹⁷ ICT stands for “Information and Communication Technologies,” which are “technolo-

and limits to digital surveillance of private user data.¹⁸ Many others, however, remain silent.¹⁹ This Note argues that Congress should compel ICTs to make a standardized disclosure when the government requests data. ICTs would be required to publicly disclose whether or not they published a chart on their company website showing detailed information about the number and nature of government requests for data on a country-by-country basis.

The Securities and Exchange Commission (“SEC”) is the agency tasked with overseeing corporate disclosures.²⁰ Because most ICTs are registered with and report to the SEC,²¹ it makes sense to add the

gies that provide access to information through telecommunications. It is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication mediums.” *ICT*, TECHTERMS.COM, <http://www.techterms.com/definition/ict> (last visited Mar. 17, 2015).

¹⁸ See *Open Letter to Washington*, *supra* note 1. On December 9, 2013, AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo launched “ReformGovernmentSurveillance.com” and issued an Open Letter to Washington urging limits to digital surveillance and government accountability. Press Release, Microsoft, Tech Company Coalition Supports Global Surveillance Principles, Calls on US to Lead Reform Efforts (Dec. 9, 2013), *available at* <http://news.microsoft.com/2013/12/09/tech-company-coalition-supports-global-surveillance-principles-calls-on-us-to-lead-reform-efforts/> [hereinafter *Open Letter Press Release*]; see also *Open Letter to Washington*, *supra* note 1. The letter stated: “For our part, we are focused on keeping users’ data secure—deploying the latest encryption technology to prevent unauthorized surveillance on our networks, and by pushing back on government requests to ensure that they are legal and reasonable in scope.” *Open Letter Press Release*. Furthermore, they called upon “the US to take the lead and make reforms that ensure that government surveillance efforts are clearly restricted by law, proportionate to the risks, transparent and subject to independent oversight.” *Id.* Because of historically close ties to government, see Wyatt & Miller, *supra* note 16, telecommunications companies are often more reluctant to reveal government requests for information. See, e.g., Stephen Lawson, *On Snooping Disclosures, AT&T and Internet Companies Are Like Night and Day*, PCWORLD (Dec. 6, 2013, 9:55 PM), <http://www.pcworld.com/article/2070680/on-snooping-disclosures-atandt-and-internet-companies-are-like-night-and-day.html> (noting that AT&T attempted to squash a shareholder proposal for semi-annual transparency reports on information requests for customer information from the government). Nevertheless, on December 19, 2013, Verizon announced it would begin publishing transparency reports, and the next day AT&T also pledged to produce government requests for user data reports in 2014. See Sam Gustin, *AT&T Follows Verizon with Plans for Transparency Report*, TIME (Dec. 20, 2013), <http://business.time.com/2013/12/20/att-transparency-report/>.

¹⁹ Since the 2013 Snowden leaks, there have only been a few collective ICT company appeals for surveillance reform. See, e.g., *Open Letter to Washington*, *supra* note 1; *Open Letter to the Senate*, REFORM GOVERNMENT SURVEILLANCE, <http://reformgovernmentsurveillance.com> (last visited Mar. 17, 2015); Declan McCullagh, *Silicon Valley Execs Blast SOPA in Open Letter*, CNET.COM (Dec. 14, 2011, 7:53 AM), <http://www.cnet.com/news/silicon-valley-execs-blast-sopa-in-open-letter>. Among the companies who signed these letters, only some of the Internet and tech industries’ leaders contributed, and not a single telecommunications company joined any of the letters demanding reform. *Id.*

²⁰ See Larry D. Soderquist & Theresa A. Gabaldon, *SECURITIES LAW* 124–25 (4th ed. 2011).

²¹ See *id.* at 123 (registration with the SEC is necessary “when the securities are held of

transparency disclosure to their annual Form 10-K filing with the Commission. This disclosure would take the form of a simple checklist: the ICT either checks a box confirming publication of the model disclosure chart, or checks a box indicating a deviation from the model-chart requirement. If it does the latter, it must explain its reasons for the deviation.

This comply-or-explain formula gives ICTs flexibility to adjust the chart to fit their circumstances as long as they provide situation-specific reasons for doing so. Although ICTs are given a certain amount of leeway, companies that misrepresent the accuracy or completeness of the information published to users would face SEC enforcement actions and other civil litigation such as whistleblower actions.

This Note begins with an overview of private and legislative attempts to impose transparency in government requests for data and then discusses the mechanics of SEC disclosures. Part I.A discusses Microsoft, Google, Yahoo, and other ICTs' participation in the Global Network Initiative ("GNI"), which created procedures for how ICTs should deal with government requests and developed a reporting standard incorporated into the model chart proposed by this Note. Part I.B explores the Global Online Freedom Act ("GOFA")²² and why it has failed; its defects indicate the kind of reporting requirements Congress and ICTs have refused to endorse.

In light of GOFA's failure, Part II proposes the steps Congress should take to authorize an appropriate SEC rule, drawing on successful examples included in the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank")²³ and on the comply-or-explain Code of Ethics rule included in the Sarbanes-Oxley Act of 2002.²⁴

Part III proposes model legislative language and describes how it would work in practice. This Part also responds to potential arguments against the viability of an SEC disclosure solution by underscoring the proposed rule's similarity to Dodd-Frank's successful Conflict Minerals provision and by detailing how it would avoid the

record by at least 500 persons and the issuer has total assets exceeding \$10 million," which encompasses most ICTs); *see also* Securities Exchange Act ("Exchange Act") of 1934 § 12(g)(1), 15 U.S.C. § 78l(g)(1) (2012).

²² Global Online Freedom Act of 2013 (GOFA), H.R. 491, 113th Cong. (2013).

²³ Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified as amended in scattered sections of 15 U.S.C.).

²⁴ Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 15 and 18 U.S.C.).

SEC misinterpretation issue that plagued Dodd-Frank's Extractive Industries transparency rule.

I. THE NEED FOR DISCLOSURE AND EFFORTS TO ACHIEVE IT

Both the technology industry and Congress have grappled with creating a workable and effective way to make government requests for user data more transparent, but both have come up short. This Part explores why both private initiatives like GNI and public initiatives like GOFA have failed to achieve industry-wide transparency.

A. *The Global Network Initiative: ICT Self-Regulation and the Development of a Government Requests Reporting Standard*

Following the intense 2006 debates discussed above, Microsoft, Google, and Yahoo came together to launch GNI in October 2008.²⁵ Although GNI began as a reputation-rebuilding measure and a preemptive move to forestall congressional action, the organization has since established itself as a forum for self-regulation and industry dialogue regarding Internet restriction and government requests for private user data.²⁶ GNI's successes have much to teach about what makes transparency rules effective. So do its shortcomings.

GNI is a multi-stakeholder initiative comprised of ICT leaders, civil society organizations, and academic institutions, working together to “[p]rotect[] and [a]dvanc[e] [f]reedom of [e]xpression and [p]rivacy in [i]nformation and [c]ommunications [t]echnologies.”²⁷ The GNI foundational principles recognize the need to balance two equally important considerations: (1) respecting user privacy and free speech and (2) cooperating with legitimate government requests in-

²⁵ See Larry Downes, *Why No One Will Join the Global Network Initiative*, FORBES (Mar. 30, 2011), <http://www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/> (noting that the non-profit GNI has failed to attract other tech companies in its efforts to protect privacy); Press Release, Global Network Initiative, *Diverse Coalition Launches New Effort to Respond to Government Censorship and Threats to Privacy* (Oct. 26, 2008), https://globalnetworkinitiative.org/newsandevents/Diverse_Coalition_Launches_New_Effort_To_Respond_to_Government_Censorship_and_Threats_to_Privacy.php.

²⁶ See Downes, *supra* note 25.

²⁷ GLOBAL NETWORK INITIATIVE, PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY 1, available at https://www.globalnetworkinitiative.org/sites/default/files/GNI_-_Principles_1_.pdf (last visited Mar. 17, 2015) [hereinafter GNI PRINCIPLES]; see also GLOBAL NETWORK INITIATIVE, GOVERNANCE, ACCOUNTABILITY, & LEARNING FRAMEWORK 1, available at https://globalnetworkinitiative.org/sites/default/files/GNI_-_Governance_Accountability_Learning.pdf (last visited Mar. 17, 2015) [hereinafter GNI GOVERNANCE]; *Participants*, GLOBAL NETWORK INITIATIVE, <https://globalnetworkinitiative.org/participants/index.php> (last visited Mar. 17 2015) [hereinafter *GNI Participants*].

volving “cybercrime, national security, and the safety of children online.”²⁸ ICTs work alongside civil society and academic institutions, such as Human Rights Watch²⁹ and The George Washington University Law School,³⁰ to craft human rights due diligence procedures that fit the ICT industry.³¹

One of GNI’s ICT members’ main obligations is to develop policies and procedures for handling government requests for private user data.³² The GNI Implementation Guidelines state that “[p]articipating companies will adopt policies and procedures which set out how the company will assess and respond to government demands for disclosure of personal information.”³³ Moreover, the companies are to “narrowly interpret and implement government demands that compromise privacy” and must “seek clarification or modification from authorized officials when government demands appear overbroad, unlawful . . . or inconsistent with international human rights laws and standards on privacy.”³⁴ The Guidelines also note the preferred form of requests—written demands that indicate the legal basis for the information requests, list the requesting government entity, and are signed by an authorized official³⁵—and require companies to ensure that governments “follow established domestic legal processes” when seeking user data.³⁶

²⁸ Crystal Ostrum, *To Seek, Receive, and Impart Information: Internet Restrictions in Saudi Arabia*, 9 INT’L J. CIV. SOC. L. 33, 39 (2011) (quoting GLOBAL NETWORK INITIATIVE, INAUGURAL REPORT 2010 2, available at https://globalnetworkinitiative.org/files/GNI_Annual_Report_2010.pdf).

²⁹ *GNI Participants*, *supra* note 27.

³⁰ *The George Washington University Law School Joins the Global Network Initiative*, GLOBAL NETWORK INITIATIVE (Dec. 17, 2012), <https://www.globalnetworkinitiative.org/news/george-washington-university-law-school-joins-global-network-initiative>.

³¹ See GNI PRINCIPLES, *supra* note 27, at 3.

³² GLOBAL NETWORK INITIATIVE, IMPLEMENTATION GUIDELINES FOR THE PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY 6, available at http://globalnetworkinitiative.org/sites/default/files/GNI_-_Implementation_Guidelines_1_.pdf [hereinafter GNI IMPLEMENTATION].

³³ *Id.*

³⁴ *Id.* GNI provides guidance on how to fulfill this obligation, noting that “[o]verbroad could mean, for example, where more personal information is requested than would be reasonably expected based on the asserted purpose of the request.” *Id.*

³⁵ *Id.* The application guidance recognizes that there are “certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.” *Id.*

³⁶ *Id.* at 7. This requirement also means that companies must challenge requesting governments in domestic court or obtain the assistance of other authorities when governments do not follow such processes. See *id.* (stating that it is “neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on privacy, the likelihood of success, the

Although GNI is an admirable initiative, two critical flaws prevent it from being a standalone solution to transparency. First, because GNI's work is constrained by confidentiality regarding ICT members' internal systems, due to trade secret concerns, much of GNI's compliance audits are aggregated and anonymized.³⁷ This anonymous format makes it difficult to gauge company-specific performance. Hence, there is a legal need for disclosure reform to enable ICTs to publicly furnish individualized information.³⁸

Second, even though GNI boasts an impressive roster of participants³⁹—Facebook joined in May 2013 after years of refusing partici-

severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend").

³⁷ See GLOBAL NETWORK INITIATIVE, PUBLIC REPORT ON THE INDEPENDENT ASSESSMENT PROCESS FOR GOOGLE, MICROSOFT, AND YAHOO 15–20 (2014), available at <https://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf> [hereinafter GNI PUBLIC REPORT]. The report states that information on ICT members' compliance is aggregated and anonymized "to allow public disclosure of important information that might otherwise raise confidentiality concerns or have unintended consequences." *Id.* at 15.

³⁸ Even when ICTs want to voluntarily disclose individualized data, they sometimes meet governmentally-imposed obstacles. See *id.* at 20 ("Google, Microsoft, and Yahoo have filed suit with the FISA Court seeking the right to share data with the public on the number of FISA requests they receive, and all three companies have publicly supported legislation that would make it possible for companies to report on FISA requests."). In January 2014, the Department of Justice settled with Google, Microsoft, and Yahoo, relaxing the rules on what FISA information these companies could disclose. Larry Zeltzer, *US Govt, Tech Firms Settle: Round 1 to the Govt*, ZDNET (Jan. 27, 2014), <http://www.zdnet.com/article/us-govt-tech-firms-settle-round-1-to-the-govt/>; *Twitter Sues FBI, DOJ to Release More Info About Government Surveillance*, CBS NEWS (last updated Oct. 7, 2014, 6:33 PM), <http://www.cbsnews.com/news/twitter-sues-fbi-doj-to-release-more-info-about-government-surveillance/>. These "relaxed rules" require companies to report the "number of requests in increments of 1,000, and [they] can only report the data with a six-month delay" See *Tech Companies Give First Look at Secret Gov't Data Requests*, CBS NEWS (Feb. 3, 2014, 4:34 PM), <http://www.cbsnews.com/news/google-microsoft-yahoo-facebook-linked-in-secret-government-nsa-data-requests/>. Although these FISA transparency wins are encouraging, they alone are not enough because there are other categories of legal authority upon which governments request user data that should also be subject to open disclosure. See *infra* Part III.

³⁹ See GNI PARTICIPANTS, *supra* note 27. GNI ICT members include Google, Facebook, LinkedIn, Microsoft, Yahoo, and ProCera Networks. *Id.* GNI also began a two-year collaboration with Alcatel-Lucent, France Telecom-Orange, Nokia Siemens Network, Vodafone, and Telefonica, among others. *Key Telecommunications Players Collaborate with the Global Network Initiative on Freedom of Expression and Privacy Rights*, Global Network Initiative (Mar. 12, 2013), <https://www.globalnetworkinitiative.org/news/key-telecommunications-players-collaborate-global-network-initiative-freedom-expression-and-privacy-rights/>. GNI investment company members include Folksam, Walden Asset Management, Trillium Asset Management, F&C Investments, EIRIS Conflict Risk Network, Domini Social Investments, Church of Sweden, Calvert Investments, and Boston Common Asset Management. GNI PARTICIPANTS, *supra* note 27.

pation⁴⁰ and LinkedIn joined in March 2014 after serving as an observer since 2013⁴¹—some important and influential ICTs simply refuse to join. Twitter and Apple, for example, have notoriously refrained from joining GNI.⁴² Another non-GNI member, Cisco Technology Systems, presents a more troublesome example. In 2011, Cisco faced two lawsuits in U.S. federal court, both related to its sale of technology to the Chinese government which then allegedly used the technology to target dissidents.⁴³ Presently, Cisco does not publish any type of government requests transparency report on its website.⁴⁴

Some lawmakers, such as Senator Richard Durbin, have routinely called out tech and telecom companies, such as Cisco and AT&T, for their failure to self-regulate through GNI.⁴⁵ One observer remarked,

⁴⁰ *Facebook Joins the Global Network Initiative*, GLOBAL NETWORK INITIATIVE (May 22, 2013), <https://globalnetworkinitiative.org/news/facebook-joins-global-network-initiative>.

⁴¹ *LinkedIn Joins the Global Network Initiative*, GLOBAL NETWORK INITIATIVE (Mar. 24, 2014), <https://globalnetworkinitiative.org/news/linkedin-joins-global-network-initiative>.

⁴² See Downes, *supra* note 25 (noting that Senator Richard Durbin has written to the CEO of Twitter “demanding that [he] sign on to the self-regulating GNI”); Michael Keller, *The Apple ‘Kill List’: What Your iPhone Doesn’t Want You to Type*, DAILY BEAST (July 16, 2014), <http://www.thedailybeast.com/articles/2013/07/16/the-apple-kill-list-what-your-iphone-doesn-t-want-you-to-type.html> (quoting Jillian York, Electronic Frontier Foundation’s Director for International Freedom of Expression who stated that “Apple is one of the most censorious companies out there” and who “cited the company’s history of censoring products in its App Store and its lack of participation in the Global Network Initiative, a nonprofit partnership between Google, Yahoo, Microsoft, and a number of human-rights groups and other organizations advocating for free expression online”).

⁴³ Deji Olukotun, *Human Rights Verdict Could Affect Cisco in China*, GLOBAL VOICES ONLINE (Apr. 24, 2013), <http://advocacy.globalvoicesonline.org/2013/04/24/human-rights-verdict-could-affect-cisco-in-china/>. One case involved practitioners of Falun Gong, a religion with over two million members in China, who accused “Cisco of marketing its technology to construct the Golden Shield, or what is popularly called the Great Firewall of China, while knowing that its products would be used to target dissidents.” *Id.* The second case alleged that the Chinese government targeted online bloggers and other activists by using Cisco’s “Great Firewall” censors. *Id.* These suits were subsequently dismissed in 2014. See *Cisco Systems Lawsuits (re China)*, BUS. & HUM. RTS. RESOURCE CTR., <http://business-humanrights.org/en/cisco-systems-lawsuits-re-china> (last visited Mar. 17, 2015).

⁴⁴ Instead, Cisco provides links to its General Counsel Mark Chandler’s blog post, “Cisco Supports Freedom of Expression, an Open Internet and Human Rights” which states that Cisco supports free expression on the Internet, and to its Corporate Social Responsibility documents. See Mark Chandler, *Cisco Supports Freedom of Expression, an Open Internet and Human Rights*, CISCO BLOG (June 6, 2011), <http://blogs.cisco.com/news/cisco-supports-freedom-of-expression-an-open-internet-and-human-rights/>. The 2013 Cisco Corporate Social Responsibility Annual Report notes that the company complies with government requests for disclosures but does not participate in the PRISM program. *Corporate Social Responsibility*, CISCO.COM, <http://csr.cisco.com/pages/csr-reports> (last visited Mar. 17, 2015); *2013 Corporate Social Responsibility Report*, at B13, B19, http://www.cisco.com/assets/csr/pdf/CSR_Report_2013.pdf.

⁴⁵ See Press Release, Senator Richard Durbin, Durbin, Coburn Continue to Press Tech Companies on Human Rights Code of Conduct (Aug. 7, 2009), <http://www.Durbin.Senate.Gov/>

“[b]ehind all of the prodding to join [GNI], of course, is the explicit threat that if GNI doesn’t succeed in self-regulating the relationship between tech companies and repressive governments, Washington stands ready to regulate.”⁴⁶ Similarly, Senator Durbin declared that if “U.S. companies are unwilling to take reasonable steps to protect human rights, Congress must step in.”⁴⁷ His proclamation, however, stands against a background of failed attempts to legislate ICT transparency.

B. Failed Legislation: The Global Online Freedom Act

Over the last seven years, New Jersey Representative Chris Smith has pushed GOFA as the answer to calls for greater ICT transparency regarding government demands.⁴⁸ Originally, GOFA set up a disclosure and penalty system that held American ICTs accountable for aiding and abetting information and privacy breaches.⁴⁹ The bill, however, did not get past committee when it was first introduced in 2006.⁵⁰ None of GOFA’s subsequent versions, including the most recent 2013 bill, have made it out of the House either—even though the last two versions had dropped the civil and criminal penalty provision.⁵¹ GOFA is unlikely to ever pass because it suffers both hypocrisy and ambiguity. Any effective legislation must learn from GOFA’s flaws and overcome them.

GOFA aims to:

[P]revent United States businesses from cooperating with repressive governments in transforming the Internet into a tool of censorship and surveillance, to fulfill the responsibility of the United States Government to promote freedom of expression on the Internet, to restore public confidence in the

Public/Index.Cfm/Pressreleases?ID=47879b56-3081-4adb-85f7-77ae8ee0bec2; Press Release, Senator Richard Durbin, Durbin Sends Letter to Technology Firms Regarding Internet Freedom in China (Feb. 2, 2010), <http://www.durbin.senate.gov/public/index.cfm/pressreleases?ID=17305a4c-c7b7-4006-acfe-789ec72007df>.

⁴⁶ Downes, *supra* note 25.

⁴⁷ Senator Dick Durbin, *Tyrants Can Use Facebook, Too*, POLITICO (Mar. 7, 2011), available at <http://www.durbin.senate.gov/public/index.cfm/statementscommentary?ID=13d1f560-1cc7-41d2-b670-667bd59130df>.

⁴⁸ GOFA was first introduced in 2006, GOFA, H.R. 4780, 109th Cong. (2006), then reintroduced in 2007, GOFA, H.R. 275, 110th Cong. (2007). It was introduced again in 2009, GOFA, H.R. 2271, 111th Cong. (2009); in 2011, GOFA, H.R. 3605, 112th Cong. (2011); and in 2013, GOFA, H.R. 491, 113th Cong. (2013).

⁴⁹ See H.R. 4780.

⁵⁰ *Id.*

⁵¹ See H.R. 491; H.R. 3605.

integrity of United States businesses, and for other purposes.⁵²

It tries to achieve this by requiring “U.S.-listed Internet Communications Services companies operating in Internet-restricting countries to include in their annual reports [to the SEC] information on company policies on human rights due diligence.”⁵³

GOFA’s framework elicits two primary points of contention. The first frequently cited deficiency is the ambiguity with which GOFA defines key requirements.⁵⁴ One of those requirements is the disclosure of its “human rights due diligence” report.⁵⁵ GOFA mandates that a company’s annual report to the SEC include any company policies that relate to human rights due diligence and indicate whether it states the company’s “expectations of personnel, business partners, and other parties under the control of the company.”⁵⁶ Although GOFA’s mission is to curb governmental Internet restriction and privacy breaches, under this vague definition, a company could simply file a report affirming that it exercises “human rights due diligence.” The company could, in essence, fulfill what is supposed to be a rigorous reporting requirement by, for example, quoting from its employee ethics handbook and listing personnel trained in privacy and human rights, without revealing just how (and how many times in the past year) it confronted government requests for user data or shutdowns.

An even more ambiguous term is “internet communications service company.”⁵⁷ GOFA requires each “internet communications service company” that operates in an Internet-restricting country to include in its annual report the due diligence information noted above.⁵⁸ GOFA defines the designation as a business that provides “electronic communication services or remote computing services” and that is required to submit an annual report to the SEC.⁵⁹ Although exceptions are carved out for companies in lodging, transportation, food services, and banking,⁶⁰ this broad definition could

⁵² H.R. 491.

⁵³ Ian Brown, *The Global Online Freedom Act*, 14 GEO. J. INT’L. AFF. 153, 156 (2013).

⁵⁴ Grant Gross, *Critics Question Wording of Internet Freedom Bill*, PCWORLD (Apr. 10, 2013), <http://www.pcworld.com/article/2033773/critics-question-wording-of-internet-freedom-bill.html>.

⁵⁵ H.R. 491 § 201(a).

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ *Id.*

nevertheless capture small U.S. companies providing computing and electronic services. This would mean that the companies would be forced to register with the SEC although they have never gone public. Such an over-inclusive application could therefore impose severe filing requirements on companies that have never even traded on a stock exchange.

Second, the State Department's electronic-surveillance reporting is potentially problematic. It is hypocritical for an agency of the executive branch to be the sole decision maker regarding which countries qualify as "Internet-restricting" when the Snowden disclosures showed that the executive branch has itself been an egregious privacy violator.⁶¹ The solution to the executive branch's information lockup, as the tech giants' *Open Letter to Washington* suggested,⁶² is greater transparency by the U.S. government, not increased executive discretion—especially given the post-Snowden findings. Furthermore, GOFA limits human rights due diligence disclosures only to "Internet-restricting countries."⁶³ Consequently, GOFA potentially excludes valuable reporting on countries such as India or Thailand that, while they engage in some form of content bans, may not be considered "Internet-restricting."⁶⁴

Unlike the manageable, subject-specific Dodd-Frank disclosures discussed below,⁶⁵ GOFA tries to tackle both Internet censorship and surveillance, resulting in legislation that is too unwieldy and burdensome to pass. GOFA's decisive flaw is that it sets up a nebulous "human rights due diligence" requirement that asks companies to disclose only policies and procedures regarding government demands—not concrete data such as the number, nature, and percentage of requests granted. As explained further in Part III, for any future trans-

⁶¹ Eaton, *supra* note 11; Surya Deva, *Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?*, 39 GEO. WASH. INT'L L. REV. 255, 315–16 (2007) ("[S]ome provisions of the [Global Online] Freedom Act are simply impractical, unworkable, or overly ambitious. The U.S. President has been empowered to designate annually Internet-restricting countries. Although this concept is central to the success of the Act, there is a possibility that this power could be misused for political gains. Whereas States friendly with the U.S. administration may escape such designation, some other States might be classified as Internet-restricting countries just because they are not on good terms with the administration." (internal quotation marks omitted)). Although Deva's article refers to the 2006 version of GOFA, the provision empowering the executive branch to classify Internet-restricting countries has remained. See H.R. 491 § 104(a) ("[T]he Secretary of State shall designate Internet-restricting countries for purposes of this Act.").

⁶² See *Open Letter to Washington*, *supra* note 1.

⁶³ See H.R. 491 § 201.

⁶⁴ See Brown, *supra* note 53, at 158.

⁶⁵ *Infra* Part II.A.

parency legislation to be effective and approved by Congress, it must both (1) tailor disclosure to the data that ICTs are willing and ready to furnish in response to government requests, and (2) make reporting easy in order to facilitate compliance.

II. A USEFUL FRAMEWORK: THE SEC AND “COMPLY-OR-EXPLAIN” DISCLOSURES

Instead of pushing comprehensive legislation such as GOFA that attempts to police both Internet privacy and information restriction, Congress should enact a more focused measure that heeds consumer and tech company complaints.⁶⁶ The recent *Open Letter to Washington* demonstrates that industry leaders—often archrivals—actually agree on something: the need for action on transparency.⁶⁷ Legislation that compels catalogued government requests based on models from current industry leaders is more likely to be successful because the form and substance of the disclosures are drawn from the ICT sector itself.⁶⁸

One way to achieve uniform transparency disclosures across the ICT industry is to use the SEC to facilitate the process. This Part outlines the SEC’s current disclosure process. First, Part II.A explains how Congress empowers the SEC to promulgate rules. Part II.A.1 illustrates how the SEC sometimes misinterprets that authorization using Dodd-Frank’s Extractive Industries disclosure as an example, and Part II.A.2 discusses Dodd-Frank’s Conflict Minerals provision, which provides an example of an effective SEC disclosure rule. Second, Part II.B explores a unique disclosure style called “comply-or-

⁶⁶ Information/site-blocking is a more difficult issue and not one on which tech leaders generally agree. Google determined that its operations in China, for example, necessitated a certain amount of information filtering at the behest of Beijing. See Brenkert, *supra* note 10, at 454. However, Twitter determined that it would block a user’s account at the request of a government within that country while allowing people outside of the country to see the tweets. See Emily Greenhouse, *Twitter’s Speech Problem: Hashtags and Hate*, NEW YORKER (Jan. 25, 2013), <http://www.newyorker.com/news/news-desk/twitters-speech-problem-hashtags-and-hate>. Legislation that ties the two separate issues of government demands for data and information restriction risks reform in the former due to disagreement of best practices in the latter. This is why this Note argues that any successful congressional action moving forward needs to tackle the problems separately and steer clear of a “one-bill-fits-all” approach.

⁶⁷ See *Open Letter to Washington*, *supra* note 1 (“Transparency is essential to a debate over governments’ surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly disclose this data publicly.”).

⁶⁸ See *infra* note 164 and accompanying text; see also *infra* Appendix, Transparency Report Screenshots.

explain,” which is widely used in European corporate governance and could provide a middle ground solution to the government requests disclosure issue.

A. *The SEC: A Vehicle for Public Disclosure*

The SEC was created under the Securities and Exchange Act of 1934 (“Exchange Act”)⁶⁹ and has the authority to make rules to execute securities laws.⁷⁰ Sometimes, Congress requires the SEC to make rules according to its own specifications,⁷¹ which is usually accomplished via legislative amendment to the Exchange Act. Thus, Congress “both makes its own law . . . and gives the Commission guidance for rulemaking.”⁷² Section 13(a) of the Exchange Act is the provision that lists the disclosure filings required by the Commission.⁷³ By registering securities on a U.S. stock exchange, a company becomes “[an issuer] subject to the periodic reporting requirements of section 13(a).”⁷⁴ Often, Congress’s statutory authorization to the SEC as to how the Commission should carry out its own agency mandate is ambiguous,⁷⁵ which leaves the SEC to determine the legislative intent regarding the appropriate level of public disclosure.

1. *Dodd-Frank’s Extractive Industry Provision: What Not to Do*

Recent litigation over the SEC’s implementation of Dodd-Frank section 1504, the Extractive Industries disclosure provision,⁷⁶ illustrates the challenges that the SEC sometimes faces in determining legislative intent while developing rules.⁷⁷ The SEC’s Extractive Industries Provision, partly influenced by the disclosure framework developed by the Extractive Industries Transparency Initiative,⁷⁸ a

⁶⁹ Securities Exchange Act of 1934 (“Exchange Act”), Pub. L. 73-291, 48 Stat. 881 (codified at 15 U.S.C. § 78 et seq.).

⁷⁰ See SODERQUIST & GABALDON, *supra* note 20, at 14. Section 19(a) of the Securities Act of 1933, for example, states that “[t]he Commission shall have authority from time to time to make . . . such rules and regulations as may be necessary to carry out the provisions of this title” *Id.*

⁷¹ *Id.*

⁷² *Id.*

⁷³ *Id.* at 124 (“Under [section 13(a)], the Commission has power to require the filing of virtually any document or report it wishes.”).

⁷⁴ *Id.* Registration with the SEC is required when securities are held by at least 500 people and the issuer has total assets greater than \$10 million. *Id.* at 123; Exchange Act § 12(g)(1)).

⁷⁵ *Id.* at 14 (noting that while Congress at times has given the SEC guidance for its rules, “[i]n other situations, Congress has chosen simply to turn everything over to the Commission”).

⁷⁶ Dodd-Frank § 1504, codified at 15 U.S.C. § 78m(q) (2012).

⁷⁷ See *Am. Petroleum Inst. v. SEC*, 953 F. Supp. 2d 5 (D.D.C. 2013).

⁷⁸ *Id.* at 9, 25.

self-regulatory organization similar to GNI, requires the SEC to develop rules that compel “reporting issuers engaged in the commercial development of oil, natural gas, or minerals to disclose in an annual report certain payments made to the United States or a foreign government.”⁷⁹ Further, the rules must require that the “information [is] provided in an interactive data format, and the Commission must make a compilation of the [government payments] information available online.”⁸⁰

On the basis of the rules developed pursuant to this provision, oil, natural gas, and mining company associations brought suit against the SEC in the District Court for the District of Columbia, claiming that the SEC misinterpreted Congress’s directive in two ways.⁸¹ First, the associations contended the SEC erroneously interpreted the statute to require the SEC to publish the companies’ annual reports without redacting any confidential information.⁸² Second, the industry groups argued the Commission arbitrarily and capriciously denied reporting exemptions for certain countries that prohibit the disclosure of payment information.⁸³ The SEC received comments that suggested the SEC provide exemptions for four countries—Angola, Cameroon, China, and Qatar—because a forced withdrawal from those four countries might result in losses in the billions, but the SEC nevertheless ignored their exemption proposal.⁸⁴

Adopting the oil, gas, and mining groups’ interpretation of the disclosure rule, the court held that the SEC misinterpreted Dodd-Frank’s directive.⁸⁵ The court determined that the SEC’s refusal to redact any financial information was erroneous.⁸⁶ The court rejected the SEC’s argument that Congress “unambiguously required public disclosure of the issuers’ annual reports.”⁸⁷ Thus, because the SEC

⁷⁹ See SEC, SPECIALIZED CORPORATE DISCLOSURE, www.sec.gov/spotlight/dodd-frank/speccorpdisclosure.shtml (last updated May 30, 2013).

⁸⁰ *Id.*

⁸¹ *Am. Petroleum Inst.*, 953 F. Supp. 2d at 11.

⁸² See *id.* at 11–12. The SEC received many comments suggesting that it “mak[e] public only a compilation of [the] information” but decided not to adhere to these comments as it “believe[d] Section 13(q) requires resource extraction issuers to provide the payment disclosure publicly and does not contemplate confidential submissions of the required information.” *Id.* at 12 (internal quotation marks omitted).

⁸³ *Id.* at 11.

⁸⁴ *Id.* at 21.

⁸⁵ *Id.* at 11.

⁸⁶ *Id.*

⁸⁷ *Id.* at 13 (internal quotation marks omitted).

erroneously determined that it was required to promulgate this regulation based on legislative intent, the court found the rule invalid.⁸⁸

The court also found that the SEC's refusal to grant any exemption for the four countries was arbitrary and capricious.⁸⁹ Noting that "no legislation pursues its purposes at all costs,"⁹⁰ the court reminded the SEC that Congress "allow[ed] the aims of specific statutes to yield to practicality" and allowed for exemptions for some provisions including 13(q).⁹¹ Thus, it rejected the SEC's argument that "adopting such an exemption would be inconsistent with the structure and language of Section 13(q)"⁹² and found its refusal to consider exemptions was arbitrary and capricious.⁹³ In the end, it is ultimately the Commission's duty to weigh competitive burdens, such as reporting costs and public interest considerations, when a proposed rule raises those concerns.⁹⁴

The foregoing overview of SEC rulemaking and of interpretive mishaps underscores three important points. First, the SEC is Congress's main vehicle for regulating public dissemination of important private sector information. Second, the SEC often has discretion to interpret the legislative mandate. Third, although the SEC is a valuable institution for gaining insight into corporate practices, if the Commission does not engage in a reasoned consideration of economic consequences and other competitive burdens of reporting, then it risks judicial adjudication of its institutional rulemaking competency. These are important points to consider when deciding the language and scope of a transparency measure tackling government requests for user data.

⁸⁸ *Id.* at 20 ("An agency regulation must be declared invalid, even though the agency might be able to adopt the regulation in the exercise of its discretion, if it was not based on the agency's own judgment but rather on the unjustified assumption that it was Congress' judgment that such a regulation is desirable or required." (internal quotation marks omitted)).

⁸⁹ *Id.*

⁹⁰ *Id.* at 22 (quoting *Rodriguez v. United States*, 480 U.S. 522, 525–26 (1987)).

⁹¹ *Id.*

⁹² *Id.* at 10.

⁹³ *Id.* at 23.

⁹⁴ See *SODERQUIST & GABALDON*, *supra* note 20, at 122–23 ("When engaged in rulemaking, or the review of a rule . . . the Commission [must] consider whether the action will promote efficiency, competition, and capital formation, at any time it is required to consider or determine whether an action is necessary or appropriate in the public interest." (internal quotation marks omitted)); see also 15 U.S.C. § 78w(a)(2) (2012) (the SEC "shall not adopt any such rule or regulation which would impose a burden on competition not necessary or appropriate.").

2. *Dodd-Frank's Conflict Minerals Disclosure: A Lesson in Implementation*

One of Dodd-Frank's other specialized transparency provisions mandates disclosures for companies using "conflict minerals" coming from the Democratic Republic of the Congo ("DRC").⁹⁵ The Conflict Minerals rule is illustrative of the kind of tailored, subject-specific SEC disclosure rule that Congress has been willing to approve.⁹⁶ It highlights two important points, one on process and the other on purpose: (1) the SEC's cost-benefit analysis is more likely to withstand attack if the Commission thoroughly considers stakeholders' objections to certain aspects of the rule and tweaks the disclosures to alleviate competition concerns; and (2) the more specific the congressional directive, the less the chance that the SEC will misinterpret its mandate.

Congress designed the Conflict Minerals provision to stop U.S. firms from financing violence in the DRC.⁹⁷ The statute calls upon the SEC to adopt regulations "requiring companies that use 'conflict minerals' that are 'necessary to the functionality or production' of their products . . . to disclose to the Commission whether those minerals originated in the DRC or an adjoining country."⁹⁸ Although industry groups challenged the rule as being arbitrary and capricious, the court upheld the Commission's implementation of the Conflict Minerals rule.⁹⁹ SEC's promulgation of this rule serves as an example of the type of reasoned execution found lacking in the Extractive Industries case.

There are two reasons why the court did not vacate the Commission's implementation of the Conflict Minerals rule as it did the Ex-

⁹⁵ See 17 C.F.R. §§ 240, 249(b); *Nat'l Ass'n Mfrs. v. SEC*, 956 F. Supp. 2d 43, 46 (D.D.C. 2013) *aff'd in part, rev'd in part*, 748 F.3d 359 (D.C. Cir. 2014) (reversing only on the First Amendment challenge to the "non DRC conflict free" language, otherwise the decision was affirmed). This Note's solution is not affected by the First Amendment ruling because the model disclosure does not impose any labels on ICTs nor does it force ICTs to self-label in any way.

⁹⁶ See 17 C.F.R. §§ 240, 249(b).

⁹⁷ See Dodd-Frank § 1502 (codified at 15 U.S.C. § 78m(p) (2012)). Congress asserted that "the exploitation and trade of conflict minerals originating in the [DRC] is helping to finance conflict characterized by extreme levels of violence in the eastern [DRC], particularly sexual- and gender-based violence, and contributing to an emergency humanitarian situation." Dodd-Frank § 1502(a). The Congressional Record reveals that senators believed an SEC disclosure scheme would help to promote responsible mineral sourcing, and serve as a step towards eradicating the conflict minerals issue. See, e.g., 156 CONG. REC. S3976 (daily ed. May 19, 2010) (statement of Sen. Feingold).

⁹⁸ *Nat'l Ass'n Mfrs.*, 956 F. Supp. 2d at 47; 15 U.S.C. § 78m(p)(1)(A), (2)(B).

⁹⁹ See *Nat'l Ass'n Mfrs.*, 956 F. Supp. 2d at 46.

tractive Industries rule.¹⁰⁰ First, the SEC's Adopting Release not only considered reporting and competition cost estimates from a diverse set of investing stakeholders, but also responded with its own cost-benefit calculations to balance the commentators' economic concerns with Congress's directive.¹⁰¹ Although the Extractive Industries' Adopting Release also included discussions on the impact on competition and economic burdens on issuers,¹⁰² the Commission there dismissed stakeholders' estimates without a satisfactory explanation.¹⁰³ Here, on the other hand, the Commission took steps to adjust its proposed rule after stakeholders raised objections. For example, one of the SEC's cost-benefit modifications arose from the recognition that the statute "could be interpreted to apply to a wide range of private companies not previously subject to [the SEC's] disclosure and reporting rules."¹⁰⁴ The Commission concluded that the more "reasonable" interpretation was to limit the application of the rule to those companies that must file annual reports with the SEC.¹⁰⁵ Thus, the instances of SEC cost-benefit adjustments are evidence of the kinds of measured consideration that the Commission should undertake when promulgating a rule derived from a congressional directive.

The second reason why the court upheld the SEC's implementation here was because the agency adhered to "a permissible construction of the statute."¹⁰⁶ Unlike the Commission's analysis of the Extractive Industries rule, where the SEC advanced the implausible argument that Congress unambiguously compelled it to publish issuers' unredacted payment disclosures,¹⁰⁷ here the Commission "deployed traditional tools of statutory construction . . . looking to

¹⁰⁰ See *supra* Part II.A.1.

¹⁰¹ *Nat'l Ass'n Mfrs.*, 956 F. Supp. 2d at 59–60 ("Upon receiving four separate cost estimates from commentators . . . the Commission noted the 'wide divergence' among the various analyses, ranging from \$387 million to \$16 billion As set forth in the Adopting Release, the Commission believed that a 'combination of the analyses [would] provide a useful framework for understanding various cost components,' and it 'strive[d] to achieve a balanced and reasonable analysis based on the data and assumptions provided by all commentators, as well as [the Commission's] own analysis and assumptions' . . . [T]he SEC took 'into account the views expressed in other comment letters, and made modifications to the analyses provided by the manufacturing industry association and university group commentators accordingly.' . . . This methodology strikes the Court as eminently appropriate").

¹⁰² See *Disclosure of Payments by Resource Extraction Issuers*, 77 Fed. Reg. 56,398–413 (Sept. 12, 2012).

¹⁰³ *Am. Petroleum Inst. v. SEC*, 953 F. Supp. 2d 5, 21–23 (D.D.C. 2013).

¹⁰⁴ See *Conflict Minerals*, 77 Fed. Reg. 56285 (Sept. 12, 2012).

¹⁰⁵ *Nat'l Ass'n Mfrs.*, 956 F. Supp. 2d at 48.

¹⁰⁶ *Chevron, U.S.A., Inc. v. Natural Res. Def. Council*, 467 U.S. 837, 843 (1984).

¹⁰⁷ See *supra* notes 86–88 and accompanying text.

congressional intent and legislative history” to determine the statute’s purpose.¹⁰⁸ Whereas the SEC constructed the Extractive Industries disclosure rule to “pursue[] its purposes at all costs,”¹⁰⁹ the Commission adjusted the Conflict Minerals rule to be “proportionate to the interests sought to be advanced.”¹¹⁰ Determining what interests are sought, however, can be a difficult task for an agency if all it has to work with is a vague directive. Therefore, if Congress provides guidance on implementing a rule before delegating the task to an agency, the agency’s task will be narrowed and its uncertainty regarding the rule’s formulation decreased. In reviewing the Conflict Minerals disclosure, for example, the court noted that the “express, statutory directive *from Congress* . . . was driven by *Congress’s determination* that the due diligence and disclosure requirements it enacted would help to promote peace and security in the DRC.”¹¹¹ Rather than “second-guess[ing] Congress’s judgment as to the benefits of disclosure,” the SEC thus only had to concern itself with “promulgat[ing] a rule that would promote the benefits Congress identified and that would hew closely to that congressional command.”¹¹²

The main takeaway from the discussion of Dodd-Frank’s specialized disclosures is that process and purpose are two frequent pitfalls for implementing agencies. To avoid process defects, the SEC should engage in a cost-benefit analysis that (1) weighs the impact of a disclosure rule on competition¹¹³ and (2) thoroughly addresses commentators’ objections and issuers’ interests.¹¹⁴ Congress, on the other hand, controls the purpose of any given policy objective. The more explicitly Congress conveys that objective, and thus eliminates uncertainties, the less likely that an agency will stray from the mandate.

B. Comply-or-Explain: Toward a “Hard Law” Best Practice

With the lessons from SEC rulemaking in mind, the analysis now turns to what kind of rule best captures the process and purpose aims detailed above. This Part explores a unique disclosure style called

¹⁰⁸ *Nat’l Ass’n Mfrs.*, 956 F. Supp. 2d at 64 (“[I]t is entirely appropriate for an agency, in the course of construing a statute it is charged with implementing, to consider whether a particular interpretation is consistent with the statute’s purpose.”).

¹⁰⁹ *Am. Petroleum Inst. v. SEC*, 953 F. Supp. 2d 5, 22 (D.D.C. 2013) (quoting *Rodriguez v. United States*, 480 U.S. 522, 525–26 (1987)).

¹¹⁰ *Nat’l Ass’n Mfrs.*, 956 F. Supp. 2d at 81 (internal quotation marks omitted).

¹¹¹ *Id.* at 58.

¹¹² *Id.* (internal quotation marks omitted).

¹¹³ *Id.* at 58–59.

¹¹⁴ *Id.* at 66.

“comply-or-explain.” Although it is popular in a European corporate context, comply-or-explain is less ubiquitous in the United States.¹¹⁵ This Part first defines the disclosure style and provides an overview of its successes and failures in the European context. Second, it discusses Sarbanes-Oxley’s comply-or-explain rule and how a similar disclosure scheme would work for the ICT sector.

1. *Definition and Application in the European Corporate Context*

Beginning in the early 1990s, European countries have spearheaded comply-or-explain practices.¹¹⁶ The United Kingdom, in its 1992 Cadbury Report, was the first European country to advance comply-or-explain rules; the Report led to the development of numerous codes such as the German Cromme Code¹¹⁷ and ultimately spurred the European Commission’s 2006 adoption of a comply-or-explain code.¹¹⁸ “Comply” can mean “strict adherence to the *letter* of the code or to the underlying principle, or both.”¹¹⁹ Nonconformance through an “explain” disclosure is “generally justified by recourse to firm- or industry-level particularities.”¹²⁰ The Cromme Code, for example, recommends that each company establish an audit committee.¹²¹ If small Firm A forms such a committee, it will “comply” with the rule; if Firm A does not apply the rule because, for instance, it already has a small supervisory board so creating another small committee would be duplicative, then it will “explain” its decision.¹²² In both scenarios, Firm A fully satisfies the disclosure requirement. The “essential genius,” therefore, of comply-or-explain is that “companies

¹¹⁵ See Paul Sanderson et al., *Flexible or Not? Comply-or-Explain Principle in UK and German Corporate Governance* 13 (University of Cambridge Centre for Business Research, Working Paper No. 407, 2010) (noting that the U.K. has a “soft” best practices approach, whereas the U.S. has a “statutory” or “hard law” approach).

¹¹⁶ RiskMetrics Group et al., *Study on Monitoring and Enforcement Practices in Corporate Governance in the Member States* 22 (Sept. 23, 2009), http://ec.europa.eu/internal_market/company/docs/ecgforum/studies/comply-or-explain-090923_en.pdf. Following a series of corporate scandals—Polly Peck, BCCI, and Maxwell in the U.K., and Metallgesellschaft and Bayerische Hypo und Vereinsbank in Germany—the need for a “practical” code of corporate governance became apparent. Sanderson, *supra* note 115, at 1. The UK created a code in 1992, followed by Germany in 2002. *Id.* at 4.

¹¹⁷ See RiskMetrics Group et al., *supra* note 116, at 22–23.

¹¹⁸ Petra Inwinkl et al., *The Comply-or-Explain Principle: Stakeholders’ Views on How to Improve the “Explain” Approach* 3 (Jönköping Int’l Bus. Sch.), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2331285.

¹¹⁹ Sanderson, *supra* note 115, at 2.

¹²⁰ *Id.* at 3.

¹²¹ *Id.* at 2–3.

¹²² *Id.* at 3.

can be said to be in conformance with the code even when deviating from it.”¹²³

Although comply-or-explain’s flexibility allows firms to “fine tune” their governance to changing circumstances, the rule’s main drawback is the lack of recourse for empty explanations.¹²⁴ In his survey of reporting statistics among the top 245 publicly traded companies in the United Kingdom, Professor Antoine Faure-Grimaud discovered the following trends: (1) companies that did not comply but explained provided poor quality explanations; (2) in almost twenty percent of the instances of noncompliance, firms did not explain at all; (3) when nonconformers explained, they usually failed to provide specific justifications for noncompliance; (4) shareholders appeared indifferent to the quality of explanations of noncompliance; and (5) returns on compliers’ portfolios were not significantly greater than those of noncompliers.¹²⁵

Faure-Grimaud notes, however, that the tendency to comply or provide specific explanations increased after 2001, which may have been due to the market’s decline and the implosion of Enron and Worldcom that in turn led to heightened scrutiny of corporate governance policies.¹²⁶ This trend toward compliance is illustrated by W.M. Morrison’s governance evolution. Since the enactment of the U.K. Combined Code, the supermarket chain W.M. Morrison was consistently not in compliance with six out of eight provisions of the code, and provided either a poor or no explanation.¹²⁷ Shareholders never raised the issue of deficient explanations during the years in which company performance was high.¹²⁸ Following Morrison’s 2004 takeover of Safeway, however, company performance declined and “shareholder pressure” led to the appointment for the first time of a non-executive director, followed by four additional independent non-executive directors later in the year.¹²⁹ The Morrison case demonstrates that shareholder monitoring does not typically lead to better explanations, but rather to forced full compliance.¹³⁰

¹²³ Inwinkl, *supra* note 118, at 9.

¹²⁴ Antoine Faure-Grimaud et al., *Corporate Governance in the UK: Is the Comply-or-Explain Approach Working?*, 1–2 (Fin. Mkts. Grp., London Sch. of Econ. & Political Sci., Discussion Paper No. 581), available at http://eprints.lse.ac.uk/24673/1/dp581_Corporate_Governance_at_LSE_001.pdf.

¹²⁵ *Id.*

¹²⁶ *Id.* at 12.

¹²⁷ *Id.* at 16.

¹²⁸ *Id.*

¹²⁹ *Id.*

¹³⁰ *Id.* at 17.

Indeed, full compliance seems to be the emerging status quo among high-profile corporations in Europe.¹³¹ Professor Paul Sanderson's University of Cambridge study found that the market itself created a norm of full compliance due to real (and perceived) internal managerial tensions and external investor pressures.¹³² The threat of an "illegitimacy discount"¹³³ in the capital markets and of "adverse comment in the press on a company's compliance position"¹³⁴ has made "soft" comply-or-explain practices akin to "hard law."¹³⁵ Nevertheless, under comply-or-explain, companies technically are still free to deviate and are even encouraged to do so if it is in their best interest, as long as they provide "situation-specific" reasons.¹³⁶

2. *Sarbanes-Oxley: Comply-or-Explain in the U.S. Corporate Context*

Comply-or-explain is not an "especially common mechanism," but it "works in the context of corporate governance because the regulatees are relatively high profile and their actions are monitored by self-interested investors."¹³⁷ Although Congress has not experimented with comply-or-explain rules as much as its European counterparts, there has been at least one significant exercise of the rule in the last decade.¹³⁸

Following the Enron and WorldCom securities fraud scandals, Congress passed the Sarbanes-Oxley Act of 2002 as a way to rein in the unethical behavior occurring in some of the largest U.S. companies.¹³⁹ The main provisions of the Act set forth "minimum standards of professional conduct for securities lawyers representing issuers."¹⁴⁰ One of these new standards, for example, is that the issuers' CEOs

¹³¹ See, e.g., Sanderson, *supra* note 115, at 26–28.

¹³² *Id.* at 29, 34, 38–39. In a different 2009 study, Sanderson found that fifty-one percent of the thirty largest companies in the U.K. and forty percent of the thirty largest companies in Germany were in full compliance with the code. *Id.* at 2.

¹³³ Inwinkl, *supra* note 118, at 8 (internal quotation marks omitted).

¹³⁴ *Id.*

¹³⁵ Sanderson, *supra* note 115, at 26.

¹³⁶ See Inwinkl, *supra* note 118, at 5. In 2013, the European Commission made a recommendation to improve the quality of corporate responses. The proposed framework is still in the consultation phase. See European Commission, Enhancing the EU Corporate Governance Framework (2013) [hereinafter "EU CORPORATE GOVERNANCE"], available at http://ec.europa.eu/smartregulation/impact/planned_ia/docs/2013_markt_033_corporate_governance_framework_en.pdf.

¹³⁷ Sanderson, *supra* note 115, at 12.

¹³⁸ Sarbanes-Oxley Act, 15 U.S.C. § 7264 (2002).

¹³⁹ See SODERQUIST & GABALDON, *supra* note 20, at 24.

¹⁴⁰ *Id.*

and CFOs must certify the accuracy of annual and quarterly SEC reports.¹⁴¹ Related to the certification feature is the comply-or-explain ethics code requirement which states the SEC must issue rules that require issuers “to disclose whether or not . . . [the] issuer has adopted a code of ethics for senior financial officers”¹⁴² While companies are not required to adopt these ethics codes, they must describe why they have not done so.¹⁴³

Ten years following its enactment, Sarbanes-Oxley has generally been successful in enhancing corporate governance reporting.¹⁴⁴ Unlike the British or German codes, which lack enforcement mechanisms to ensure adequate explanations or even reporting in general,¹⁴⁵ Sarbanes-Oxley imposes a criminal penalty for knowingly or willfully filing a deficient report.¹⁴⁶ The Act’s “biggest hammer,” therefore, is “the threat of jail time for corporate executives who knowingly certify inaccurate financial reports.”¹⁴⁷ Furthermore, the Exchange Act, which governs the SEC, also imposes criminal liability for making false or misleading statements in filings to the Commission.¹⁴⁸ Although the Justice Department has remained on the sidelines, the SEC has brought “civil crisis-related false-certification charges ‘in every case in which such charges were appropriate.’”¹⁴⁹ Because of the multitude of potential enforcement actors—including the Justice Department, the SEC, shareholders, and whistleblowers¹⁵⁰—companies are under more scrutiny in the United States than abroad where there are not perhaps as many avenues to litigation.

Drawing on the lessons of what has worked in Europe and in Sarbanes-Oxley, a comply-or-explain government requests rule can compel and standardize ICT-friendly disclosures. It is clear from the *Open Letter to Washington* that tech leaders are in favor of trans-

¹⁴¹ See SODERQUIST & GABALDON, *supra* note 20, at 128.

¹⁴² 15 U.S.C. § 7264.

¹⁴³ See SODERQUIST & GABALDON, *supra* note 20, at 129.

¹⁴⁴ Michael Rapoport, *Law’s Big Weapon Sits Idle*, WALL ST. J. (July 29, 2012, 7:48 PM), <http://online.wsj.com/news/articles/SB10000872396390444130304577557190343517170>.

¹⁴⁵ See Faure-Grimaud, *supra* note 124, at 1–2.

¹⁴⁶ 15 U.S.C. § 1350.

¹⁴⁷ Rapoport, *supra* note 144.

¹⁴⁸ See SODERQUIST & GABALDON, *supra* note 20, at 125.

¹⁴⁹ Rapoport, *supra* note 144 (internal quotation marks omitted).

¹⁵⁰ *Id.* (discussing Justice Department, SEC, and shareholder litigation on the basis of fraud in disclosures); Ben Kerschberg, *The Dodd-Frank Act’s Robust Whistleblowing Incentives*, FORBES (Apr. 14, 2011, 9:20 AM), <http://www.forbes.com/sites/benkerschberg/2011/04/14/the-dodd-frank-acts-robust-whistleblowing-incentives/> (explaining the whistleblower provisions under Dodd-Frank).

parency, but only on their terms—for example, they state that governments should allow for the publication of the “nature and number” of government requests for information, but not much more.¹⁵¹ Unlike the Sarbanes-Oxley disclosures, some ICT leaders are telling Congress that they *want* to publish public reports.¹⁵² In contrast to GOFA’s unwieldy human rights due diligence report,¹⁵³ the proposed comply-or-explain rule takes the form of a two-step box-checking exercise: (1) the ICT indicates whether it complied with the model chart disclosure, and if the answer is yes, there is no further requirement; and (2) if the answer is no, the company must explain why it did not conform to the model chart, citing situation-specific reasons in line with the interpretive guidance on acceptable explanations.¹⁵⁴ Furthermore, due to several enforcement avenues, this rule avoids the empty justifications defect associated with other comply-or-explain rules.

III. SEC COMPLY-OR-EXPLAIN DISCLOSURE RULE ON GOVERNMENT REQUESTS FOR USER DATA

In a recent speech to the Justice Department, President Obama proposed several reforms to NSA programs, including changing “programs and procedures . . . to provide greater transparency to [the Executive’s] surveillance activities.”¹⁵⁵ One way to achieve greater transparency of the kind that both the government and ICTs accept is to implement an SEC comply-or-explain rule. This new reporting requirement would: (1) apply only to SEC-registered companies that provide telecommunications, internet, or computing services for a fee or to the general public for free; (2) compel solely general, nonconfidential information on the number and nature of government requests for user data that the ICTs receive; (3) standardize the disclosure form in the ICT industry by detailing the Transparency Report’s chart organization and by sorting the requests into different categories to provide the most accurate accounting of government demands; and (4) employ a comply-or-explain structure that a company can satisfy by merely checking the box indicating that it published the Trans-

¹⁵¹ See *Open Letter to Washington*, *supra* note 1.

¹⁵² See *id.*

¹⁵³ See H.R. 491.

¹⁵⁴ See *infra* Part III.

¹⁵⁵ President Barack Obama, Speech on NSA Reforms at the Department of Justice (Jan. 17, 2014) (transcript available at http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html).

parency Report on its website or by explaining in situation-specific terms why it chose not to publish any report or an incomplete one.

This Part outlines the proposed rule in three phases. First, it explains to whom the SEC rule applies and how this rule's definition remedies GOFA's main defect. Second, it provides the disclosure's structure, comparing this model's cost-effectiveness to that of the Dodd-Frank provisions and contrasting it to GOFA's elaborate human rights due diligence report. Finally, it outlines the pragmatic recommendations given to ICTs that choose to explain, referring back to the lessons from the European comply-or-explain experience.

A. "ICT Company" Defined

One of GOFA's defects is its ambiguous definition of "Internet communications service company."¹⁵⁶ The bill defined these companies as businesses that are required to file SEC reports and provide "electronic communications services or remote computing services."¹⁵⁷ This definition is under-inclusive because it does not include telecommunications companies. It is also over-inclusive because it captures a "publicly traded company [along with its subsidiaries and suppliers] offering cloud computing service or website hosting services . . . even if its servers are exclusively located in the U.S., so long as the services could be used by members of the public in an Internet restricting country."¹⁵⁸

The disclosure statute outlined below solves this problem in two ways. First, in amending the Exchange Act to delegate the administration of disclosures to the SEC, the definition of "Information and Communications Technology Company" must clearly state that it applies only to firms that charge a fee for service, such as AT&T, but also to firms providing their services for free to the general public, such as Google. The disclosures would therefore not apply to firms, such as banks or hotels, that happen to provide these Internet and communications services as a by-product of their primary line of business. This avoids an over-inclusive application that imposes severe filing requirements on companies that have never even traded on a

¹⁵⁶ See H.R. 491 § 201(a).

¹⁵⁷ *Id.*

¹⁵⁸ Todd C. Taylor, *Proposed Global Online Freedom Act Could Impact Supply Chains, Outsourcing Efforts and Foreign Operations of U.S. and Multinational Companies*, BLOOMBERG LAW (Jan. 19, 2012), <http://www.bna.com/proposed-global-online-freedom-act/>. Although this article refers to the 2011 version of the bill, the definition in the 2013 bill explicitly includes "remote computing services" in the definition of "Internet communications company." Therefore, the observation still applies.

stock exchange. Second, the proposed disclosure rule would limit a firm's reporting duty only to the main ICT parent company and its wholly owned subsidiaries. An ICT company would need to report only government requests received by a partially owned subsidiary if (1) the ICT parent is a controlling shareholder (controls more than fifty percent of shares) *and* (2) the ICT parent holds a majority of director positions on the subsidiary's board of directors. The company would not in any case, however, have to worry about monitoring its suppliers' government requests activity.

Although some critics might point to the supplier and partially owned subsidiary limitations as loopholes susceptible to ICT company abuse, a pragmatic line must be drawn when it comes to the activity for which the firm will have to answer. It might be that an ICT company's supplier or partially owned subsidiary provides a requesting government with user data through non-legal avenues. This, however, is a reality in the hyper connected, technological world of today. Because legislation that "pursues its purposes at all costs"¹⁵⁹ is bound to fail,¹⁶⁰ Congress must sometimes yield to practicality when it comes to line-drawing. In the end, it does not make sense to sacrifice an entire transparency endeavor over a supplier or partially owned subsidiary exclusion.

B. Transparency Report: Government Requests Chart in Form and Substance

Although GOFA attempts to limit its application to "Internet-restricting countries,"¹⁶¹ the hypocrisy of having a U.S. executive agency designate which countries qualify under such a term is evident.¹⁶² This Note, therefore, proposes a Transparency Report that organizes the nature and number of government demands for user data using a chart composed of an alphabetical list of all countries that contacted an ICT firm in the given reporting year. No country is excluded.

Departing from GOFA's cumbersome human rights due diligence report requirements,¹⁶³ the proposed disclosure rule asks firms to compile their own transparency report in the form of a chart which

¹⁵⁹ *Rodriguez v. United States*, 480 U.S. 522, 525–26 (1987).

¹⁶⁰ *Id.* at 526 ("It frustrates rather than effectuates legislative intent simplistically to assume that *whatever* furthers the statute's primary objective must be the law.").

¹⁶¹ See H.R. 491 § 101.

¹⁶² See *supra* Part I.B.

¹⁶³ H.R. 491 § 201(a).

they must post on their company website.¹⁶⁴ The rule also includes certain specific categories by which to sort the number and nature information of user data requests. The model chart would (1) list countries in alphabetical order and indicate the number of government requests for a given reporting period (e.g., six months¹⁶⁵); (2) indicate the legal nature of the request (e.g., Search Warrant, Subpoena, Emergency Disclosure, Wiretap Order, Pen Register Order¹⁶⁶); (3) specify whether a legal basis was cognizable,¹⁶⁷ and, if not, whether the company resent the request for more information; (4) denote whether the company submitted the request to court review when the requests had no legal basis;¹⁶⁸ (5) indicate whether the users in question were notified of the government request for data;¹⁶⁹ and (6) list the percentage of requests where some user information was granted.¹⁷⁰ This approach not only draws from current industry practice¹⁷¹ but also incorporates the GNI “legal basis” framework,¹⁷² and thus by combining those factors the solution requires ICTs to disclose more than a generalized snapshot of governments’ user request activity.

There are two main counterarguments to the inclusion of the “legal basis” categories. First, some might point to increased costs in having to keep track of the legal bases on which governments base their demands for user info. This, however, is a weak argument. Most likely once an ICT company receives a government request for user

¹⁶⁴ The standard chart is modeled on a combination of Google, Facebook, Microsoft, and Twitter’s transparency reports. See *Transparency Report*, GOOGLE.COM, <http://www.google.com/transparencyreport/userdatarequests/countries/> (last visited Mar. 14, 2015); *Global Government Requests Report*, FACEBOOK.COM, https://www.facebook.com/about/government_requests (last visited Mar. 14, 2015); *Transparency Report: Information Requests*, TWITTER.COM, <https://transparency.twitter.com/information-requests/2013/jan-jun> (last visited Mar. 14, 2015); *Law Enforcement Requests Report*, MICROSOFT.COM, <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/> (last visited Mar. 14, 2015). Furthermore, the proposed rule indicates that the report will also be published on the SEC website. See *infra* Appendix. So that a company cannot bury the information in its website, the disclosure must be named “Transparency Report” and turn up as a result using general search terms such as “Government requests + company name.” *Id.*

¹⁶⁵ See, e.g., Google’s *Transparency Report*, *supra* note 164 and *infra* Appendix.

¹⁶⁶ Category labels are taken from different ICT companies’ existing chart designations. See *supra* note 164 and accompanying text.

¹⁶⁷ See GNI IMPLEMENTATION, *supra* note 27, at 6–7.

¹⁶⁸ *Id.* at 7.

¹⁶⁹ *Id.*

¹⁷⁰ See Facebook’s *Global Government Requests Report*, *supra* note 164; see also *infra* Appendix.

¹⁷¹ See *supra* note 164 and accompanying text; see also *infra* Appendix.

¹⁷² See GNI IMPLEMENTATION, *supra* note 27.

data, it then records the request electronically if the request itself is not already in electronic format.¹⁷³ Electronic records, therefore, should not significantly increase costs to companies.

Further, while there surely will be reporting costs as with all other disclosure items included in a company's annual 10-K submitted to the SEC, the costs should be substantially less under this proposed rule than under the current framework. The cost to the company of categorizing a request as a "Warrant" or "Wiretap Order" is not as burdensome as perhaps denoting it a "human rights due diligence" report conducted by an independent third party under GOFA because these categorizations involve little discretion on the part of employees.¹⁷⁴ Also, unlike Dodd-Frank's Extractive Industries Provision's disclosure rules on payments made to governments,¹⁷⁵ this Note's proposed rule only asks companies to generally label the demands, not to furnish specific facts about the legal basis asserted in every single request.

Second, some might argue that incorporating a part of the GNI framework into legislation unfairly favors one stakeholder organization and imposes a GNI standard on non-GNI participants. Congress, however, is the designated policymaker in our system of government,¹⁷⁶ which means that it can choose to codify one particular group's framework and not another. This is exactly what Congress did when it enacted Dodd-Frank's Extractive Industries Provision, as it in part based the disclosure rule on the Extractive Industries Transparency Initiative's guidelines.¹⁷⁷

Finally, some might ask why Congress should pass this proposed model disclosure if tech giants such as Google, Facebook, and Microsoft, which touch the lives of millions of users around the globe, already regularly publish reports on government requests. That argument misses the point of this Note's compel-and-standardize goal for two reasons. First, although Internet companies have led the reform

¹⁷³ Sometimes governments might make an informal oral request or a paper request, such as a warrant. See GNI PUBLIC REPORT, *supra* note 37, at 9. An ICT could easily then record this information electronically.

¹⁷⁴ See H.R. 491 § 201(a).

¹⁷⁵ See *supra* Part I.A.1.

¹⁷⁶ See *Nat'l Ass'n Mfrs. v. SEC*, 956 F. Supp. 2d 43, 79 (D.D.C. 2013) (noting that Congress has "traditional legislative authority to make predictive judgments" (internal quotation marks omitted)).

¹⁷⁷ See *Am. Petroleum Inst. v. SEC*, 953 F. Supp. 2d 5, 9 (D.D.C. 2013); see also *Disclosure of Payments Made by Resource Extraction Issuers*, 77 Fed. Reg. 56365, 56366–67 (Sept. 12, 2012) (amending 17 C.F.R. § 240.13q-1); 15 U.S.C. § 78m(q) (noting that the term "payment" should be defined "to the extent practicable" with reference to the EITI).

initiatives pushing public disclosure, far fewer telecom companies have voiced support for such reporting.¹⁷⁸ The proposed SEC disclosure, therefore, would reach more companies and compel them to adopt the transparency standard. Second, even though some of the industry's largest players already conform to a reporting model, there is no uniform standard.¹⁷⁹ Google, for example, provides the most detailed level of reporting on government requests.¹⁸⁰ Facebook, on the other hand, provides only country names and percentages without distinguishing among the types of requests with any labels.¹⁸¹

Leaders in both the Internet and telecommunications sectors agree there is a government requests transparency gap that must be filled.¹⁸² By modeling its proposed rule after the transparency reports already in use by the ICT industry,¹⁸³ this Note takes firm interests into account in both substance and form. Not only would the report be cost-effective and easy to implement, but it also takes a step forward toward normalizing government accountability to the public through surveillance practices.

C. Interpretive Guidance on “Explain”

This Note has argued¹⁸⁴ that the comply-or-explain rules could be used to make disclosure company-friendly. As previously mentioned, comply-or-explain rules reject a one-size-fits-all approach and provide companies with the flexibility to model their reporting on a set standard or to deviate from that model when the business situation demands it.¹⁸⁵ An ICT company can, therefore, meet the proposed SEC disclosure rule by either checking the box indicating it complied with the chart details above or by explaining why it chose not to disclose government requests data. The rule would mandate that a company choosing to explain its lack of disclosure must furnish specific reasons for doing so—statements like “It was our business judgment not to disclose” or “It was not in the best interest of the company” would be considered insufficient. Rather, adequate explanations should present concrete reasons for not complying, or for only partially complying. For example, an explanation that a company “did not receive requests

¹⁷⁸ See *supra* note 19.

¹⁷⁹ See *infra* Appendix. The graphs demonstrate companies' different reporting styles.

¹⁸⁰ *Id.*

¹⁸¹ *Id.*

¹⁸² See *Open Letter to Washington*, *supra* note 1; Gustin, *supra* note 19.

¹⁸³ See *supra* note 164 and *infra* Appendix.

¹⁸⁴ See *supra* Part II.B.

¹⁸⁵ See *supra* Part II.B.1.

during this reporting period from countries X, Y, or Z” or “could only comply for some but not others because governments X, Y, and Z requested the company not share the information” are simple, fact-based explanations for not fully complying with the disclosure requirement that would satisfy this rule.

Imperative to the successful operation of the comply-or-explain mechanism is interpretive guidance delineating the substance of explanations. Europeans have noted that insufficient explanations, combined with shareholders’ lack of attention to these poor explanations, are a significant weakness of a comply-or-explain reporting system.¹⁸⁶ Although the EU corporate governance setup lacks centralized enforcement, ICT companies listed on U.S. stock exchanges potentially face SEC enforcement actions, shareholder derivative suits, and other civil litigation such as whistleblower actions if they misrepresent the accuracy or completeness of information published to users.¹⁸⁷ Further, including sample situation-specific explanations in the rule itself will significantly reduce any uncertainty underlying the level of detail required.

CONCLUSION

A flexible SEC rule for government requests meets the twin aims of satisfying ICTs’ desire to supply the public with information while setting a precedent of government accountability for the future. The ICT giants’ *Open Letter to Washington* reproached governments for “tipp[ing]” the balance “too far in favor of the state and away from the rights of the individual.”¹⁸⁸ A disclosure rule that compels ICTs to publicly report on their activities with U.S. agencies and foreign governments is a first step in equilibrating that balance.

¹⁸⁶ See Faure-Grimaud, *supra* note 124, at 8, 15–16.

¹⁸⁷ See *supra* Part II.B.2.

¹⁸⁸ See *Open Letter to Washington*, *supra* note 1.

APPENDIX
PROPOSED MODEL STATUTE

DISCLOSURE OF GOVERNMENT REQUESTS FOR PRIVATE USER DATA BY INFORMATION & TECHNOLOGY COMPANIES.¹⁸⁹

Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m) is amended by adding at the end the following:

“(x) DISCLOSURE OF GOVERNMENT REQUESTS FOR PRIVATE USER DATA BY INFORMATION & TECHNOLOGY COMPANIES—

“(1) **DEFINITIONS**—In this subsection—

“(A) the term ‘information and communications technology’ includes Internet, information technology, telecommunications (fixed, mobile, and wireless telephony), software, audiovisual system, or other like areas providing electronic communications or computing services, as determined by the Commission;

“(B) the term ‘information and communications technology issuer’ means an issuer that—

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

“(ii) engages in electronic communications or computing services as described above for a fee or to the general public for free;

“(C) the term ‘Model Transparency Report’ means an electronic disclosure chart in which government requests for private user data information are identified using a uniform classification standard; and

“(D) the term ‘uniform classification standard’ means a standardized list of categories that organize government requests information included in the annual report of an information and communications technology issuer.

“(E) the terms ‘government requests’ or ‘government requests for private user data’ mean written or oral demands received by an information and communications technology issuer from a governmental agency, its officers, or agents asking for a user’s (1) personally identifiable information or (2) other Internet and computing information. Furthermore, ‘government’ includes the government of the United States as well as foreign governments.

“(2) **DISCLOSURE**—

“(A) **INFORMATION REQUIRED**—Not later than 270 days after the date of enactment of this amendment, the Commission shall

¹⁸⁹ Modeled on the text of Dodd-Frank’s Extractive Industries Provision, 15 U.S.C. § 78m(q).

issue final rules that require each information and communications technology issuer to include in an annual report: (1) any government requests for private user information received by the company; (2) any government requests received by a wholly-owned subsidiary; (3) any government requests received by a partially owned subsidiary if the parent-issuer is *both* (a) majority shareholder (51% +) *and* (b) controls a majority of positions on the board of directors—

“(B) **CONSULTATION IN RULEMAKING**—In issuing rules under subparagraph (A), the Commission may consult with any agency or entity that the Commission determines is relevant.

“(C) **MODEL TRANSPARENCY REPORT**—The rules issued under subparagraph (A) shall require that the information included in the annual report of an information and communications technology issuer be submitted in an interactive chart format, organized by country name in alphabetical order.

“(D) **UNIFORM CLASSIFICATION STANDARD**—

“(i) **IN GENERAL**—The rules issued under subparagraph (A) shall establish an interactive data standard for the information included in the annual report of an information and communications technology issuer.

“(ii) **ELECTRONIC TAGS**—The interactive data standard shall include electronic tags that identify the number and nature of requests made by a foreign government or the Federal Government to an information and communications technology issuer—

“(I) the total amounts of the government requests, by legal nature category;

Foreign Intelligence Requests

National Security Requests

Search Warrant

Subpoena

Other Court Order

Wiretap Order

Pen Register Order

Emergency Disclosures

“(II) the total amounts of the government requests that included a legally cognizable basis;

“(III) the total amounts of requests presented to the government for more information for lack of a legal basis;

“(IV) the total amounts of government requests submitted to a court for review;

“(V) the total percentage of users notified of the government requests for their private data; and

“(VI) the total percentage of requests where the issuer granted some private user information.

“(E) **INTERNATIONAL TRANSPARENCY EFFORTS**—To the extent practicable, the rules issued under subparagraph (A) shall support the commitment of the Federal Government to international transparency promotion efforts relating to government requests for user data.

“(F) **EFFECTIVE DATE**—With respect to each information and technology issuer, the final rules issued under subparagraph (A) shall take effect on the date on which the information and technology issuer is required to submit an annual report relating to the fiscal year of the information and technology issuer that ends not earlier than 1 year after the date on which the Commission issues final rules under subparagraph (A).

“(G) **PUBLIC AVAILABILITY OF INFORMATION**—

“(i) **IN GENERAL**—To the extent practicable, the Commission shall make available online, to the public, the issuer’s Transparency Report required to be submitted under the rules issued under paragraph (2)(A). Moreover, the information and technology issuers shall make available the Transparency Report, which must turn up under at least these three search terms: (1) “Government requests + company name”; (2) “Government requests for data + company name”; (3) “Transparency Report + Company name.”

“(ii) **OTHER INFORMATION**—Nothing in this paragraph shall require the Commission to make available online information other than the information required to be submitted under the rules issued under paragraph (2)(A).

“(iii) **AUTHORIZATION OF APPROPRIATIONS**—There are authorized to be appropriated to the Commission such sums as may be necessary to carry out this subsection.

“(H) **PENALTIES**—

“(i) **IN GENERAL**—The issuers reporting under this section will be subject to civil penalties for knowingly filing a deficient Transparency Report. Furthermore, under section 32 of the Securities and Exchange Act of 1934, an issuer may face criminal liability for making false statements or misrepresentations in its annual report to the Commission.

PROPOSED REGULATORY RULE**SEC IMPLEMENTING RULE FOR § 13(x)¹⁹⁰****DISCLOSURE OF GOVERNMENT REQUESTS FOR PRIVATE USER DATA BY INFORMATION & TECHNOLOGY COMPANIES**

(i) Did the information and communications technology issuer's Transparency Report **COMPLY** with the requirements of sections: **2(A); 2(C); 2(D)(i)–(ii)(I)–(VI); and 2(G)** of 13(x) **DISCLOSURE OF GOVERNMENT REQUESTS FOR PRIVATE USER DATA BY INFORMATION & TECHNOLOGY COMPANIES**?

(ii) If the information and communications technology issuer *did not* conform to those sections, explain the deviations below.

Acceptable explanations must include situation-specific reasons for deviating from the model Transparency Chart.

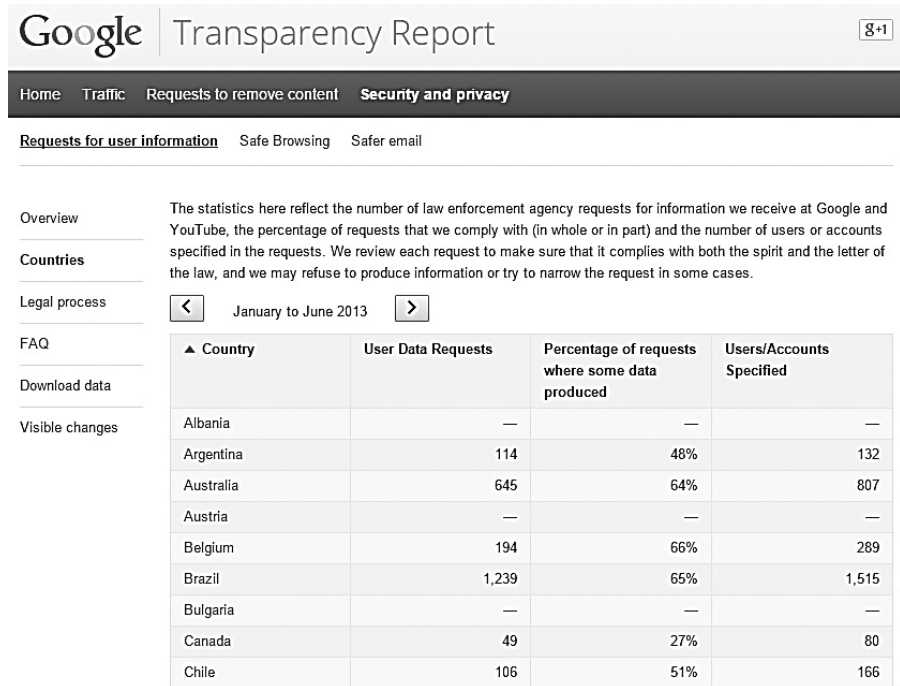
Vague statements, such as “It was in our best business judgment not to disclose” or “Current company circumstances necessitate non-disclosure,” are insufficient and

Adequate explanations present concrete reasons for nonconformance or for partial conformance. For example, “We did not receive requests during this reporting period from countries X, Y, or Z” or “We could only comply for some but not others because governments X, Y, and Z requested we not share the information” are simple, fact-based explanations for not fully complying with the disclosure rule.

¹⁹⁰ This is a draft of the rule that the SEC could use to implement the proposed Congressional mandate in § 13(x) above.

ILLUSTRATING THE NEED FOR STANDARDIZATION: SCREENSHOTS OF ICT TRANSPARENCY REPORTS¹⁹¹

FIGURE 1. SCREENSHOTS OF GOOGLE'S TRANSPARENCY REPORT¹⁹²



¹⁹¹ The screenshots included in this section have been taken from the respective company's websites. The screenshots depict the content of those webpages *exactly* as they appeared on the dates indicated in the accompanying footnote in order to demonstrate the nonstandard nature of disclosure and transparency reporting methods.

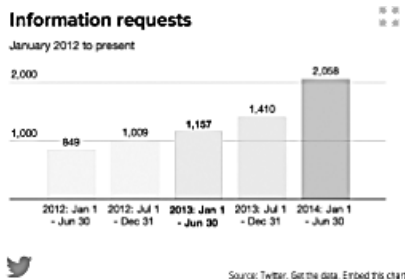
¹⁹² See *Transparency Report*, GOOGLE.COM, <http://www.google.com/transparencyreport/userdatarequests/countries/?p=2013-06> (last visited Mar. 14, 2015); *United States*, GOOGLE.COM, <https://www.google.com/transparencyreport/userdatarequests/US/> (last visited Mar. 14, 2015).

FIGURE 2. SCREENSHOTS OF TWITTER'S TRANSPARENCY REPORT¹⁹³

Information requests include worldwide government requests we've received for account information, typically in connection with criminal investigations.

The latest report includes the number of government requests received for account information, as well as the percentage of requests we complied with in whole or in part. We also mark countries in which we have received emergency disclosure requests only with an asterisk.

We have received inquiries from 8 new countries since our last report, bringing the grand total to 54 countries since the inception of our Transparency Report.



Latest report: Information requests

January 1 - June 30, 2014

Country	Account information requests	Percentage where some information produced	Accounts specified
Albania	1	0%	1
Argentina	7	0%	8
Australia	2*	100%	2
Austria	-	-	-
Bahrain	1*	0%	1

United States

Information Requests

Report	Total information requests	Non-emergency requests	Emergency requests	Percentage where some information produced	Accounts specified
2014: Jan 1 - Jun 30	1,257	1,125	132	72%	1,918
2013: Jul 1 - Dec 31	833	733	100	69%	1,323
2013: Jan 1 - Jun 30	902	-	-	67%	1,319
2012: Jul 1 - Dec 31	815	-	-	69%	1,145
2012: Jan 1 - Jun 30	679	-	-	75%	948
TOTAL	4,486	-	-	70%	6,653

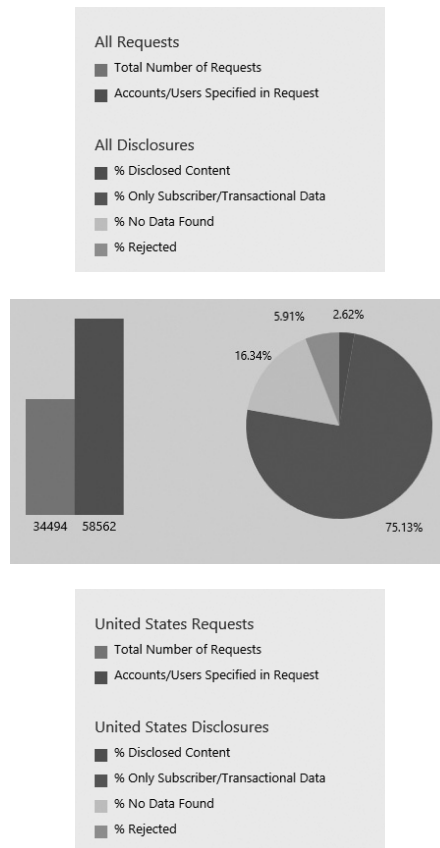
NOTE: The data in these reports is as accurate as possible, but may not be 100% comprehensive.

¹⁹³ *Information Requests*, TWITTER.COM, <https://transparency.twitter.com/information-requests/2014/jan-jun> (last visited Feb. 28, 2015); *United States*, TWITTER.COM, <https://transparency.twitter.com/country/us> (last visited Mar. 14, 2015).

FIGURE 3: SCREENSHOTS OF MICROSOFT'S TRANSPARENCY REPORT¹⁹⁴

2014 (JAN-JUN)	2013 (JUL-DEC)	2013 (JAN-JUN)					
All	Argentina	Armenia	Australia	Austria	Belarus	Belgium	Bosnia And Herzegovina
Brazil	British Virgin Islands	Bulgaria	Canada	Chile	China	Colombia	Costa Rica
Croatia	Cyprus	Czech Republic	Denmark	Dominican Republic	Ecuador	Egypt	El Salvador
Estonia	Finland	France	French Polynesia	French Southern Territories	Germany	Greece	Hong Kong
Hungary	Iceland	India	Ireland	Israel	Italy	Japan	Korea
Latvia	Liechtenstein	Lithuania	Luxembourg	Malaysia	Malta	Mexico	Moldova
Monaco	Montenegro	Netherlands	New Zealand	Norway	Pakistan	Panama	Paraguay
Peru	Poland	Portugal	Puerto Rico	Qatar	Russia	Russian Federation	Sierra Leone
Singapore	Slovakia	Slovenia	South Africa	South Korea	Spain	Sweden	Switzerland
Taiwan	Thailand	Trinidad and Tobago	Turkey	Ukraine	United Arab Emirates	United Kingdom	United States
Uruguay	Venezuela						

NOTE - Country tile in grey color represents data is not available



¹⁹⁴ *Law Enforcement Requests Report*, MICROSOFT.COM, <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/> (last visited Mar. 14, 2015).

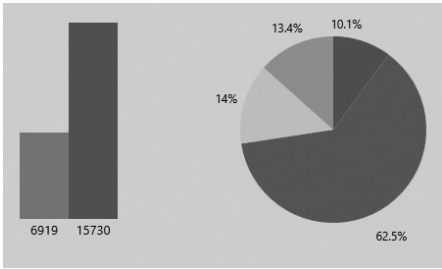


FIGURE 4: SCREENSHOT OF FACEBOOK’S TRANSPARENCY REPORT¹⁹⁵

Data Requests

Download as CSV

Country	Total Requests	Users / Accounts requested	Percentage of requests where some data produced
Albania	6	12	83 %
Argentina	152	218	27 %
Australia	546	601	64 %
Austria	35	41	17 %
Bangladesh	1	12	0 %
Barbados	3	3	0 %
Belgium	150	169	70 %
Bosnia and Herzegovina	4	11	25 %
Botswana	3	7	0 %
Brazil	715	857	33 %
Bulgaria	1	1	0 %
Cambodia	1	1	0 %
Canada	192	219	44 %
Chile	215	340	68 %
Colombia	27	41	15 %
Costa Rica	4	6	0 %
Croatia	2	2	0 %

¹⁹⁵ *Global Government Requests Report*, FACEBOOK.COM, https://www.facebook.com/about/government_requests (last visited Mar. 14, 2015).