

Improving the Transparency of Government Requests for User Data from ICT Companies

by

Amn Rahman

B.S., Computer Science, Lahore University of Management Sciences

(2014)

Submitted to the Institute for Data, Systems, and Society

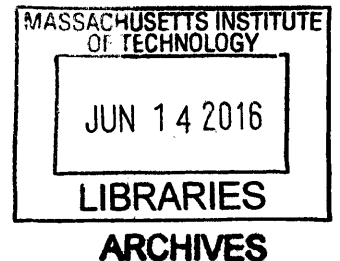
in partial fulfillment of requirements for the degree of

Master of Science in Technology and Policy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2016



© Massachusetts Institute of Technology 2016. All rights reserved.

Signature redacted

Author ...

.....
Institute of Data, Systems, and Society
May 12, 2016

Signature redacted

Certified by..

.....
Daniel J. Weitzner
Principal Research Scientist
Computer Science and Artificial Intelligence Laboratory
Thesis Supervisor

Signature redacted

Accepted by

.....
Munther Dahleh
William Coolidge Professor of Electrical Engineering and Computer Science
Director, Institute for Data, Systems, and Society
Acting Director, Technology and Policy Program

Improving the Transparency of Government Requests for User Data from ICT Companies

by

Amn Rahman

Submitted to the Institute for Data, Systems, and Society on May 12, 2016
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Technology and Policy

Abstract

In 1968, the US Congress enacted a detailed list of requirements for transparency reporting of wiretaps but with subsequent surveillance statutes with minimal reporting requirements and rapidly evolving Internet technologies, the gap in surveillance transparency grew. The Snowden disclosures in 2013 provided a peek into the surveillance landscape and the central role of ICT companies in fostering it. While attempting to salvage their tarnished reputations and encourage public discussion, several companies began to see an incentive in publishing 'transparency reports', providing statistics on user data requested by the government. Since then, publishing these reports has become a norm in the industry but the reports provide little benefit in bridging the transparency gap. The varying formats, definitions and levels of granularity in the reports and the absence of a governance framework in the industry, prevent the reports from becoming useful tools for stakeholders wishing to inform policy decisions. In addition, new technologies, modern surveillance techniques, and evolving business models have created a set of transparency requirements that is markedly different from the initial set of requirements established under the US Wiretap Act. This thesis identifies the missing elements in the current transparency reports while providing a detailed list of necessary features. In addition, it uncovers the incentives that can be leveraged using available tools to encourage better reporting practices and suggests technical, legal and policy solutions so that transparency reporting may become a useful public policy tool rather than a ritualistic practice.

Thesis Supervisor: Daniel J. Weitzner
Title: Principal Research Scientist
Computer Science and Artificial Intelligence Laboratory

Acknowledgments

I would like to dedicate this thesis to my parents for their love, prayers and support.

I am deeply grateful to my advisor, Danny Weitzner for his mentorship and for giving me the opportunity to learn from him. Ilaria Liccardi, for her support throughout what has been a very tough year. Meg Roggensack and Sarah Labowitz, for helping me appreciate and understand the complexities of this space and for taking a keen interest in my work. I would like to thank Fareed Zaffar for his invaluable guidance and support that propelled me into coming to MIT and for continuing to provide his mentorship. During these two years at MIT, I have gotten to know amazing people who have always been there to help along the way. I feel blessed to have been a part of the Technology and Policy Program and to have spent time with the faculty, administrators and my cohort who have all contributed to a truly fulfilling experience. I am indebted to Barbara DeLaBarre for her unwavering support and unfaltering energy that brightens up TPP.

Table of Contents

Chapter I: Introduction	7
Chapter II: The Wiretap Report.....	16
Chapter III: Transparency Reports	31
Chapter IV Improving Transparency Reports	50
Chapter V: Global Network Initiative	70
Chapter VI: Reducing Limitations on Transparency Reporting.....	84
Chapter VII: Recommendations	94
Bibliography	96
Appendix A	108
Appendix B	112

Chapter I

Introduction

In order for societies to function, people must give others power over themselves. Ceding Power is an inherently risky thing to do, and over the millennia we have developed a framework for protecting ourselves even as we do this: transparency, oversight, and accountability.

- Bruce Schneier

By allowing the Internet to enter our lives, we unwittingly granted power to corporate and government institutions with an insatiable appetite for the data we generate. For decades, the corporate sector assisted the government by providing access to the troves of data, facilitated by a complex network of statutes, broad interpretation of the law and little to no transparency. The business motive for collecting data in the “era of big data” aligned well with the government’s apparent need to for it to be able to “protect” the populace. The 2013 Snowden leaks cracked this alignment and created a new type of business incentive that favored transparency. These changing norms can provide better oversight of the surveillance landscape and allow the public to hold the government and the corporate sector accountable for their practices.

Background and Motivation

The Congress built a layer of surveillance transparency when it legalized the use of wiretaps in 1968 along with a detailed list of reporting requirements that were to provide the public and the Congress with information on the scale, scope and effectiveness of the wiretaps. Since then, the Administrative Office (AO) of the US Courts has been publishing statistics on the use of the wiretaps, related offenses, number of arrests, convictions, incriminating intercepts, persons intercepted, names of jurisdictions, authorizing judges, among other pieces of relevant information. The availability of these numbers provided civil society and academics a way of holding law enforcement accountable and facilitated an open discussion on surveillance in the public sphere.

With the rise of the Internet and widespread data collection by multiple companies across the globe, surveillance efforts became more focused on stored data as opposed to real time content and non-content information. A complex web of statutes emerged over the years, decentralizing and legitimizing the acquisition of data from the corporate world. Newer statutes lacked the transparency provisions of the Wiretap Act and transparency of surveillance continued to erode. The Pen Register Act of 1986 aimed at non-content real time data requires a substantially shorter transparency report providing basic information on the orders issued. The reports were intended for the public, but disappeared “into the congressional void” (Schwartz, 2008) with several instances of delayed reporting. It has only been through the diligent efforts of privacy advocates that some of the numbers have entered the public sphere (Soghoian, 2011). Schwartz called the collection of telecommunications statistics largely ritualistic and only creating a “myth of oversight” (2008).

The Stored Communications Act (SCA) introduced in 1986 provides the procedure for law enforcement access to stored content and non-content data. Official statistics for orders issued under SCA have also remained shrouded in secrecy over the past several decades. Law enforcement may also acquire information via “emergency disclosures” and no official statistics on these exist either. National security requests through National Security Letters (NSLs) and Foreign Intelligence Surveillance Act (FISA) orders remained largely secret for decades until the USA Freedom Act recently mandated reporting requirements and a few numbers have been made publicly available. These reports provide the numbers of FISA orders and NSLs that have been issued. Other than the surveillance these statutes, many other mechanisms exist in the landscape that collect data with no transparency. Schwartz calls these blank areas on the surveillance map as “semi-known unknowns” (2008) but this thesis does not address these and only looks at improving the transparency of the known mechanisms. In addition, this thesis primarily focuses on the US companies and government and therefore, steers clear of procedures that govern requests from other countries through Mutual Legal Assistance Treaties (MLATs).

The Snowden disclosures uncloaked a number of features of this landscape. Above all, it provided an understanding of how the state had been broadly interpreting the law in order to gather telephone records and Internet metadata on a large scale. Companies were accused of being complicit in facilitating the Government’s grotesque

efforts and were attacked by the public, civil society, academics and investors for not protecting the privacy of their users. In an attempt to salvage their tarnished reputations, more companies began publishing 'transparency reports' providing numbers on the requests they received from governments and the numbers they responded to. Companies and stakeholders now regard transparency reporting as a norm in the industry. The standard of reporting varies widely throughout the industry and therefore it is difficult to aggregate reports to provide a better understanding of surveillance for an informed debate.

In the absence of a governance framework in the industry to regulate and standardize these reports, stakeholders have introduced a number of methods to push companies into becoming more transparent. Some examples include the use of scorecards to grade company practices, templates to encourage more reporting, internal assessment techniques and tools to analyze current reports and practices. This thesis evaluates these tools and discusses the potential impact they may have on reporting in the future while offering a number of recommendations.

Transparency reports are also shackled by the legal limitations that govern the level of transparency they can provide. This thesis identifies the constraints that companies face due to gagging orders and laws that prevent them from disclosing the exact numbers of national security requests. In addition, it proposes policy recommendations that challenge these provisions while also encouraging government reporting of numbers to facilitate a system of two-way verifiability and accountability.

Transparency can have a real and substantial impact on policy decisions. It is important that these reports do not merely become "ritualistic" as was with the case of official statistics on telecommunications surveillance. It is easy to see that the Snowden leaks have shifted norms in a way that numbers have become important in informing policy. The aftermath of the disclosures resulted in groups imposing pressure on the Congress and the USA Freedom Act leading to an end of mass collection of records and the establishment of transparency reporting for national security requests through FISA orders and NSLs. In addition, it also provides a venue of opportunity for companies to challenge non-disclosure orders. Given the immense value that public discussion can have, it is important that efforts are made towards bridging the transparency gap.

Methodology

This thesis adopts a case-study approach to demonstrate the high level of transparency under the Wiretap Act and its erosion in the current ecosystem with decentralized surveillance and sources of data. The case study looks at the development and evolution of the reports and identifies the ways in which they can be used and have been used by stakeholders in the past.

The current landscape of corporate transparency reporting was traversed to identify the various types of reports that exist and draws out the important features that must be present in all reports. An analysis of the tools that have developed alongside these reports has been performed to identify the strengths and weaknesses of each and to predict the impact each may have on transparency reporting.

A number of stakeholders from the academia and civil liberties groups were identified based on their participation in key issues and platforms surrounding transparency reporting. These stakeholders provided their input on transparency reporting, business and human rights, multi-stakeholder platforms, and legal issues with regards to transparency. This group of stakeholders does not represent the entire range of stakeholders that is relevant to this context, but this thesis does include the opinions of a wide variety of stakeholders through publicly available interviews, workshops and discussions online. Stakeholder input was particularly critical to this thesis when evaluating tools for transparency reporting in terms of their saliency, credibility and predicted impact.

The human rights and civil liberties groups oppose threats to fundamental human rights and in this case safeguard the right of privacy. Such groups are particularly concerned about government's infringing on the citizens' right to privacy and oppose mass surveillance. Examples of such organizations are the Electronic Frontier Foundation (EFF) and the Center for Democracy and Technology (CDT) that provide amicus briefs to the courts and input to the UN Special Rapporteur on Privacy and Freedom of Expression.

Academics and experts also play a role in the debate by providing objectivity to multi-stakeholder platforms and providing analyses of the status quo. For example, GW Law participates in the Global Network Initiative (GNI), a multi-stakeholder platform in the industry. In addition, some academics may become actively involved in improving the status of transparency reporting. Harvard Berkman Center's involvement in the

creation of a Transparency Reporting Toolkit is one such example. NYU Stern Center for Business and Human Rights is another active participant in the ongoing discussions pertaining to this area.

This thesis is laced with discussions that have been conducted with various stakeholders. During the course of writing this thesis, I have been able to interview several experts from the academia and civil liberties and advocacy groups to get their thoughts on transparency reporting and what needs to be changed in order for them to be able to call them useful. The discussions centered on the transparency reports, Global Network Initiative, accountability tools such as Electronic Frontier Foundation’s (EFF) ‘Who Has Your Back?’ Report and Ranking Digital Rights’ Corporate Accountability Index, and the future of transparency. Several strengths and weaknesses of the current transparency and accountability mechanisms were identified as a result. These individuals represent a wide array of organizations and academic institutions. The following is a list of the affiliations of stakeholders interviewed along with the category they belong to. In total, there were discussions with 9 stakeholders.

Affiliation	Stakeholder Category
Georgetown Law, NYU Stern Center for Business and Human Rights, Harvard Berkman Center	Academic
Global Network Initiative, Freedom Online Coalition	Multi-stakeholder
Electronic Frontier Foundation, Human Rights Watch	Civil Liberties

Table 1. Stakeholder Affiliations

Accountability Framework

The entire transparency and accountability framework of surveillance if mapped on a graph, comprises of four nodes representing the government, companies, users and civil society. Each pair of nodes has a complex relationship where one node holds the other accountable and the direction of the arrow between them is towards the node being held to account. Companies can be held accountable by the government for violations of laws such as those governing consumer protection. In addition, the government can hold users or citizens accountable for violating the law in some way. In order to achieve this, the government may require the assistance of the company and now the company may be held accountable by the government for not assisting it. Another set of relationships that is not modeled in the diagram for the benefit of simplicity is the relationship between the congress and the law enforcement agencies. The law

enforcement agencies are accountable to the congress and some statutes require regular reports to be presented in front of the congress. Such reports may or may not be visible to the public.

Similarly, users and civil society for not respecting human rights can hold the company accountable. The development of the Internet for the most part has been free of government intervention and spearheaded by self-regulatory efforts of companies and civil society (Masiello, 2014). This resulted in a relationship in which companies are held accountable by the users and civil society through public criticism. Public criticism can be damaging for a corporate entity especially when relationships with users are based on trust. This trust if compromised, can adversely affect the success of the business. Google’s promise to not be “evil” results in a potential tradeoff between choosing something that is more profitable to shareholders and evil verses choosing something less profitable but “not evil” (Masiello, 2014). Masiello regards the promise to the public as optional. However, given the intense criticism of ICT companies after the Snowden leaks, it no longer seems optional and a company must guard its reputation and try to “do no evil”. The accountability link hence, becomes stronger. Figure 1 helps elucidate the different relationships and desired accountability between each pair of actors.

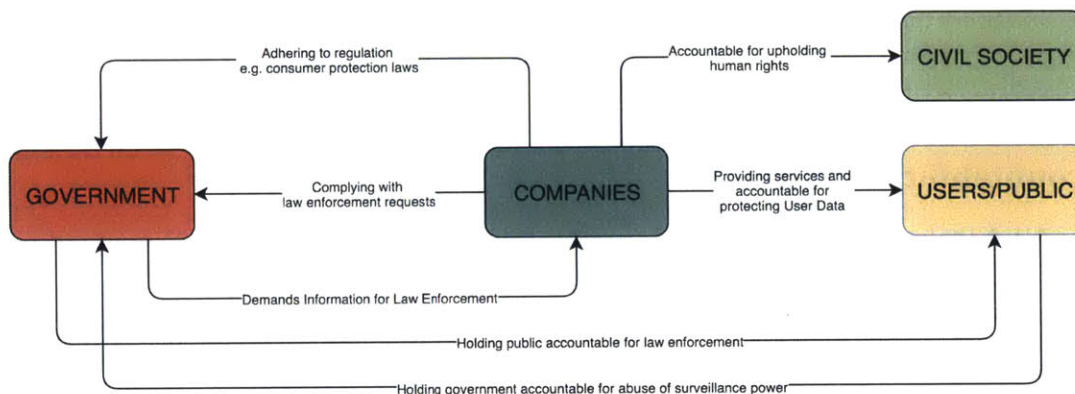


Figure 1. Accountability Framework

Accountability requires a degree transparency in the form of information regarding the internal behavior of different actors. Even with transparency, there is the need to establish metrics that allow stakeholder to compare companies on their performance in terms of transparency and privacy. This leads to the development of accountability tools

that make such analysis easier for other stakeholders. Ranking and scorecards can incentivize good policies and practices while also allowing stakeholders to compare company performance.

Related Work

Related work for this thesis comes from various directions: analysis of wiretap reports, importance and analysis of transparency reports published by ICT companies, analysis of processes that hold ICT companies accountable.

Chris Soghoian conducted an in-depth analysis of the wiretap reports in order to uncover trends from known surveillance reporting mechanisms (2011). He observed trends dealing with numbers of federal and state orders, roving authority, crimes, wiretaps of computers and email, and the instances of encryption being encountered while tapping. Soghoian conducted an analysis of reports till 2011 and was able to conclude that even with major flaws “the reports do reveal some interesting trends, such as the massive growth in the use of these metadata surveillance orders” (2012). Diffie and Landau’s book *Privacy on the Line* devotes a great deal of attention to wiretaps and also conducts an analysis on the wiretap reports and the limitations of the data (2007). Paul M. Schwartz also provides an analysis of the Wiretap Report and other telecommunication statutes while proposing recommendations for the improving the telecommunication surveillance law (2008). Schwartz regarded the numbers provided by the statutes as purely ritualistic and only creating a myth of oversight.

Transparency reporting by ICT companies is a relatively new phenomenon and there has been little academic analysis that analyzes the reports and the level of their transparency and accountability. The first ever analysis of transparency reports was conducted soon after the NSA leaks to evaluate the transparency and privacy policies of ICT companies (Kulikova, 2013) The study was based on interviews with representatives from four major Internet companies (Google, Facebook, Microsoft and Yahoo) in order to trace the motivation for the publishing the reports and their foreseen future. Kulikova describes the voluntary accountability by companies to the public as a process of self-regulation and this leads to the transparency reports and/or involvement with GNI (2013). The companies saw Google as the pioneer in the field but at the time of the study, both Facebook and Yahoo had not released their own reports but saw Google’s report as the standard to adopt (Kulikova, 2013). The study also found

that the companies were encouraged by various stakeholders pushing for greater transparency and that the reports had raised the bar of accountability practices and the NSA leaks had catalyzed the process of publishing reports (Kulikova, 2013). All the participants in the interviews felt that there was a greater need for the government to become more transparent (Kulikova, 2013).

James Losey looks at transparency reporting by tech companies as a way forward and provides a brief analysis of current practices and legal limitations but focuses more on the need for governments to become more transparent (2015).

Christopher Parsons evaluates the effectiveness of Canadian telecommunications transparency reports, by examining how they facilitate public policy goals established by civil society academics, and companies (2015). The necessity of the reports emerges from the realization that government agencies are unlikely to report on the full extent of their surveillance and even the reports the government does provide are misleading. (Parsons, 2015) The four reports released by Canadian telecom providers can provide a fuller picture of the aggregate figures on surveillance but are not completely effective in fulfilling the following policy goals: “contextualizing information about government surveillance actions, legitimizing the corporate disclosure of data about government-mandated surveillance actions, and deflecting or responding to telecommunications subscribers’ concerns about how their data is shared between companies and the government.” (2015) The inefficacy emerges from the lack of standardization, granularity, legal understanding, and policies that result in data disclosures. Similar findings have been found in other reports on Canadian telecommunication transparency spearheaded by academics.

A recent collaboration between the Berkman Center at Harvard and the Open Technology Institute, the “Transparency Reporting Toolkit” (Woolery et al., 2016), provides an industry wide survey of transparency reports and highlights the best practices in a series of memos. This publication is perhaps the most comprehensive study of transparency reports and is built over two years of research and interviews with 43 US companies.

The third stream of related research is concerned with evaluating the existing accountability mechanisms of company transparency. The Global Network Initiative (GNI) has been a subject of academic intrigue. Michael Samway goes traces the history and development of GNI as a multi-stakeholder platform and how accountability has

been incorporated into its framework (2016). Baumann-Pauly et al., compare GNI to traditional MSIs in regulating corporate conduct (2016). Older literature set goals for the GNI and pointed to the uncertainty in assessing the impact GNI may have on the industry (Maclay, 2010).

Thesis Organization

The first chapter dives into a case study of the Wiretap Report and demonstrates its usefulness over the decades and establishes its importance as the gold standard of surveillance transparency. Chapter 2 looks into the transparency reporting practices of ICT companies and identifies the current trends in reporting and the limitations that prevent the reports from becoming useful to stakeholders. The chapter also provides a detailed list of reporting requirements that companies should be encouraged to adopt. Chapter 3 looks at the various tools that stakeholders can use to incentivize and evaluate better transparency reporting practices. Chapter 4 transitions from external reporting by companies to independent assessments by multi-stakeholder initiatives (MSIs) and the role that they play by providing some transparency on internal practices of companies. Chapter 5 examines the legal limitations imposed on companies and suggests the role the government needs to play in allowing and promoting greater transparency. The thesis concludes with a summary of recommendations for companies, stakeholders, and the government.

Chapter II

The Wiretap Report

Of all the telecommunications surveillance statutes, it [The Wiretap Act] provides for the most complete accounting of behavior.

- Paul M. Schwartz

The Wiretap Report can be regarded as the “gold standard” for surveillance reporting. Had surveillance remained limited to wiretaps and pen registers, these reporting requirements and their statistics would have provided sufficient transparency on law enforcement surveillance practices (Soghoian, 2011). This chapter demonstrates the usefulness of the Wiretap Report as an accountability tool by examining the ways it can and has been used by various stakeholders and the public. In addition, the limitations of the Wiretap Report serve to highlight the need for transparency mechanisms both by the government and the corporate sector.

The legislative history of the Wiretap Act shows the intention of the Congress behind the reporting requirements in providing greater transparency of electronic surveillance:

“[The wiretap reports] are intended to form the basis for a public evaluation of its operation. The reports are not intended to include confidential material. They should be statistical in character... [they] will assure the community that the system of court-ordered electronic surveillance envisioned by the proposed chapter is properly administered and will provide a basis for evaluating its operation”¹

The first Wiretap Report, in accordance with the provisions of 18 U.S.C 2519(3) was transmitted by the Director of the Administration of the U.S. Courts to the Congress in April of 1969. The report provided a summary of the number of applications for orders authorizing or approving the interception and the number of orders and extensions granted or denied during the preceding calendar year, along with a summary and analysis of the data. It appeared in an aggregated manner at the state and county level of

¹ S. REP. 90 1097, S. Rep. No. 1097, 90TH Cong., 2ND Sess. 1968, 1968 U.S.C.C.A.N. 2112, 1968 WL 4956 (Leg.Hist.)

granularity providing a count of the number of wiretaps made for each crime, the average number of intercepts for each order, the average number of persons involved in each wiretap, the average number of incriminating intercepts, average cost of the wiretap per order, the number of persons arrested and, the number of persons convicted.

The Report also provided data at the granularity of each request. This type of table included the name of judge who authorized it, the jurisdiction, the name of the applicant, the offense, the type of wiretap, date of application, period of authorized days, extension, the number of days the wiretap lasted for, the place of (e.g. residence, business).

TABLE A.—Reports by state judges pursuant to Title 18, United States Code, Section 2519, on applications for court orders to authorize the interception of wire or oral communications—Continued

State, county and reporting number	Name of judge	Applicant	Offense specified	Kind (W) wire (O) oral	Date of application	Original period authorized (days)	Number of extensions	Total length of intercepts (days)	Place
State of New York, Kings County—Continued									
64.....	Starkey.....	Hogan.....	Kidnapping.....	W	Dec. 10, 1968	20		20	Business.
65.....	Starkey.....	Golden.....	Larceny.....	W	Dec. 19, 1968	20		20	Apartment.
66.....	Starkey.....	Golden.....	Narcotics.....	W	Dec. 24, 1968	20		20	Apartment.
67.....	Starkey.....	Golden.....	Narcotics.....	W	Dec. 24, 1968	20		20	Apartment.
68.....	Starkey.....	Golden.....	Narcotics.....	W	Dec. 24, 1968	20		20	Business.
State of New York, Onondaga County:									
1.....	Farnham.....	Gualtieri.....	Drugs.....	W	July 11, 1968	20		20	Multiple dwelling.
2.....	Farnham.....	Gualtieri.....	Drugs.....	W	Aug. 20, 1968	20		20	Residence.
3.....	Farnham.....	Gualtieri.....	Robbery.....	W	Oct. 1, 1968	20	1	40	Residence.
4.....	Farnham.....	Gualtieri.....	Gambling.....	W	Oct. 1, 1968	20		20	Market.
5.....	Farnham.....	Gualtieri.....	Gambling.....	W	Oct. 31, 1968	20		20	Residence.
6.....	Farnham.....	Gualtieri.....	Gambling.....	W	Nov. 16, 1968	20		20	Residence.
7.....	Farnham.....	Gualtieri.....	Gambling.....	W	Nov. 26, 1968	20		Not executed	Apartment.
8.....	Farnham.....	Gualtieri.....	Gambling.....	W	Nov. 26, 1968	20		20	Apartment.
9.....	Farnham.....	Gualtieri.....	Gambling.....	W	Dec. 5, 1968	20		20	Business.
10.....	Farnham.....	Gualtieri.....	Gambling.....	W	Nov. 26, 1968	20		20	Business.
11.....	Farnham.....	Gualtieri.....	Gambling.....	W	Dec. 5, 1968	20		20	Residence.
12.....	Farnham.....	Gualtieri.....	Gambling.....	W	Dec. 12, 1968	20		Not executed	Apartment.
13.....	Farnham.....	Gualtieri.....	Gambling.....	W	Dec. 12, 1968	20		20	Residence.
14.....	Farnham.....	Gualtieri.....	Gambling.....	W	Dec. 19, 1968	20		20	Apartment.
15.....	Orestein.....	Gualtieri.....	Drugs.....	W	Dec. 3, 1968	20	2	60	Multiple dwelling.

Figure 1. Snapshot from 1969 Wiretap Report

By the 1980s, the reports included summary tables and charts that captured trends over the years since the first report.

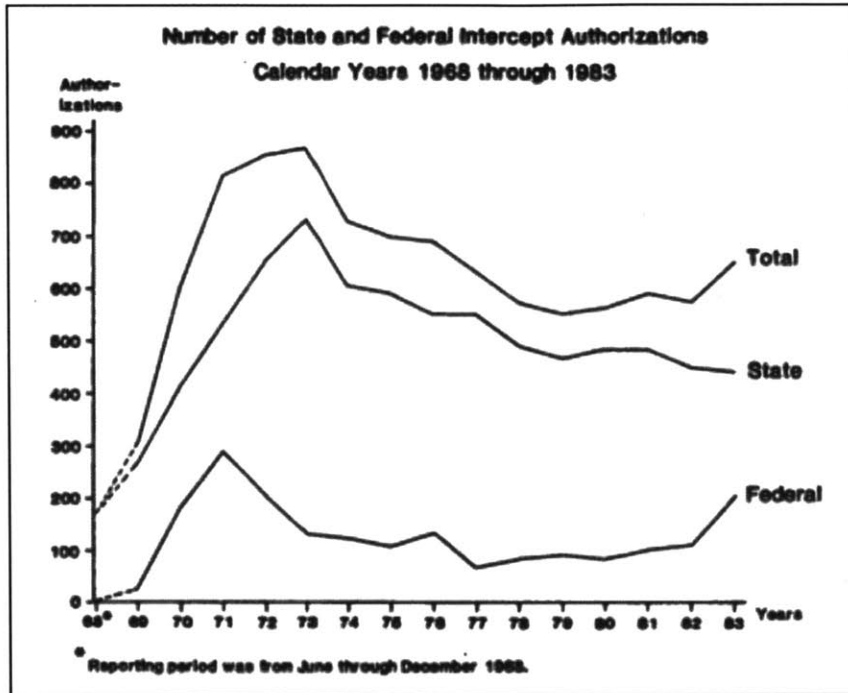


Figure 2: Snapshot from Wiretap Report 1984

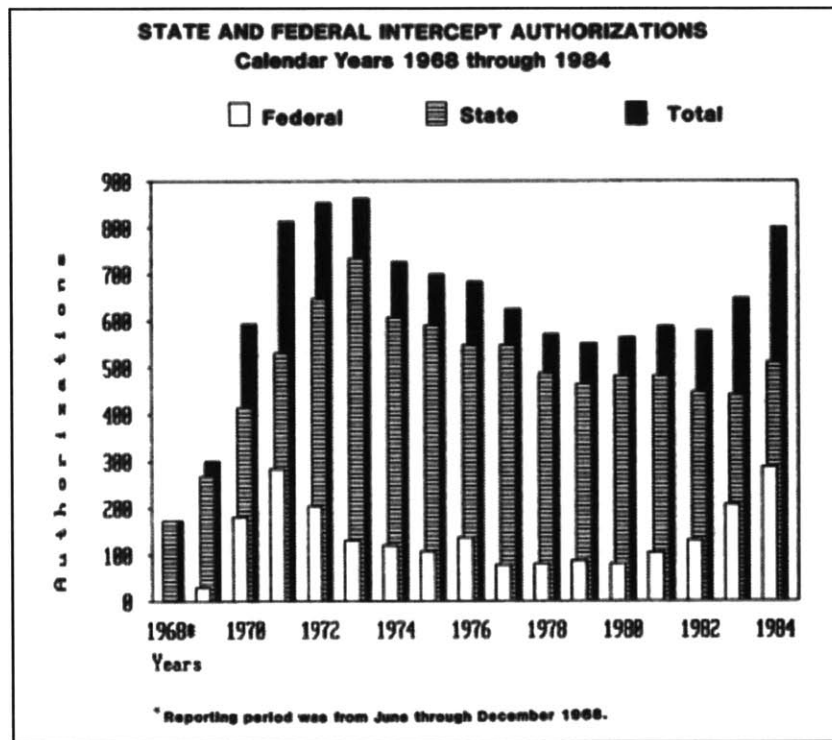


Figure 3: Snapshot from Wiretap Report 1985

While the types of data provided by the reports remained the same, the format continued to improve over the years. In 1999, Senators Leahy and Hatch proposed a bill to complement the existing reporting requirements with additional requirements

(Congressional Record, 1999). These included the number of orders where encryption was encountered and the number of instances when it prevented law enforcement access. The bill was in response to FBI Director Louis Freeh’s arguments concerning limiting the domestic use of encryption technology.

The most updated set of reports between 1997 and 2014 are available on the U.S. Courts website² while reports from previous years (1968-1996) can be obtained with some effort from online repositories such as the one maintained by HeinOnline. The reports have been available as .pdf’s, making it difficult to perform analysis at a deeper level. Since 2012, the data at the level of granularity of each order has been made available as .xls files. This is particularly important because it now provides numbers of arrests, incriminating evidence, convictions, trials, persons intercepted for each order issued in an easy to analyze format. The new type of format facilitates a number of analyses on the efficacy of the wiretaps in assisting law enforcement. A complete list of information provided under the Wiretap Report can be seen in Table 1.

Contents of the Wiretap Report 18 U.S.C. § 2511
<ul style="list-style-type: none"> • Name of authorizing judge • Name of prosecutor • Application date • State (if state order) • Jurisdiction • Number of authorized wiretaps • The number of wiretap orders that were denied • The number of wiretap orders installed, not installed, installed and not used, installed and used • Major offense identified • The average duration of the original authorization and number of extensions • The duration of the wiretap in days • The place or facility where the wiretap was authorized • The type of interception • Number of persons intercepted per installed interception device • Average number of intercepts per day • Number of interceptions per installed interception device • Number of incriminating intercepts per installed interception device • Number of intercepts per installed interception device • The total cost of interception • Cost other than manpower cost • The number of people arrested as a result of interceptions • The number of people convicted as a result of interceptions • The number of trials, motions granted, motions denied, and motions pending • Instances of encryption encountered during wiretapping and instances where it prevented access • Supplementary data from previous years that has not been reported so far

Table 1: Contents of the Wiretap Report

² AO’s webpage featuring all wiretap reports from 1997-2014: <http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports>

The need for oversight due to a history of surveillance abuse under Edgar J. Hoover and the famous case *Katz v. United States* that established wiretaps were a “search” under the Fourth Amendment led up to the Congress passing legislation for the Wiretap Act (Landau, 2011). The Act legalized wiretapping while ensuring that there was adequate transparency with regards to its use and effectiveness. However, there has been little congressional oversight over the years and there are only a few instances where the Report has resulted in some discussion. In 1996, the release of an FBI report on Future Wiretap Capacity Needs brought the wiretap reports under scrutiny though an analysis of the trends of authorization for the last 15 years (Congressional Record, 1996). The reports were criticized for missing the actual number of call content interceptions associated with each other, and the number of pen registers and trap and trace orders but was positively regarded as the only longstanding electronic surveillance source of data and a model to make projections for future design capacity for interception activity (Congressional Record, 1996). In 1999, Senator Leahy praised the AO for having “done an excellent job at preparing the wiretap reports” and proposed the addition of reporting requirements pertaining to encryption (Congressional Record, 1999). In 2004, the report’s collection procedure was highlighted in the Senate and there was a proposal to amend the reporting requirements for judges. It suggested that judges submit authorized orders to the AO at the end of every year rather than each order within 30 days of it being approved (Congressional Record, 2004). A similar proposal came up again in 2009 in the House (Congressional Record, 2009). While it appears that the Congress has paid little interest to the Report, it might just be the case that some oversight by the Congress happens behind closed doors. (Landau, 2011)

While it does not seem like the Report has had substantial utility for the Congress, it has served as an important tool for the civil society, academics and media by keeping them informed of the overall surveillance landscape. The detailed information on the wiretaps is “critical for clear decision making on surveillance law” and provides oversight (Landau, 2011). Paul M. Schwartz, regards the Wiretap Act as providing for “the most complete accounting of behavior” out of all telecommunication surveillance statutes (2008).

Chris Soghoian has conducted a number of analyses on the reports dated between 1997 and 2011 (2012) to draw out the of trends of wiretapping by federal and state law enforcement agencies. One of the advantages of conducting a similar analysis

now is that we have a dataset of three more years to look at. In addition, the AO has improved the granularity of reporting by providing a dataset featuring statistics related to each order in an easy to analyze format. While Soghoian was primarily interested in identifying the trends in the data, I'm more concerned with what needs the data can fulfill. Based on the analysis of the reports and their usage by public and civil society, the utility of the reports can be realized as important tools for transparency and accountability. In particular, the reports provide a way of knowing how the statutes are being interpreted in practice and a means of holding the law enforcement agencies accountable on claims pertaining to the effectiveness of surveillance techniques being deployed.

The scale and scope of surveillance can be deduced by the numbers of federal and state orders that are approved over time, the numbers of individuals whose communication is being intercepted, the types of crimes being addressed, the jurisdictions being targeted, and the type of communications being tapped. Figure 4 shows the changes in the number of orders issued over time and demonstrates the scale of wiretapping as a surveillance mechanism since its legalization in 1968. The number of orders rejected over time can be considered as a measure of the lack of scrutiny that is employed by judges when signing on wiretap orders. The state orders have always outnumbered the federal ones and looking into state statistics can allow civil liberties groups to hold state courts and law enforcement accountable. Figure 5 shows the number of people arrested and convicted from those who were wiretapped. However, one must be cautious when looking at these numbers and assuming a causal relationship between the wiretap and the arrests.

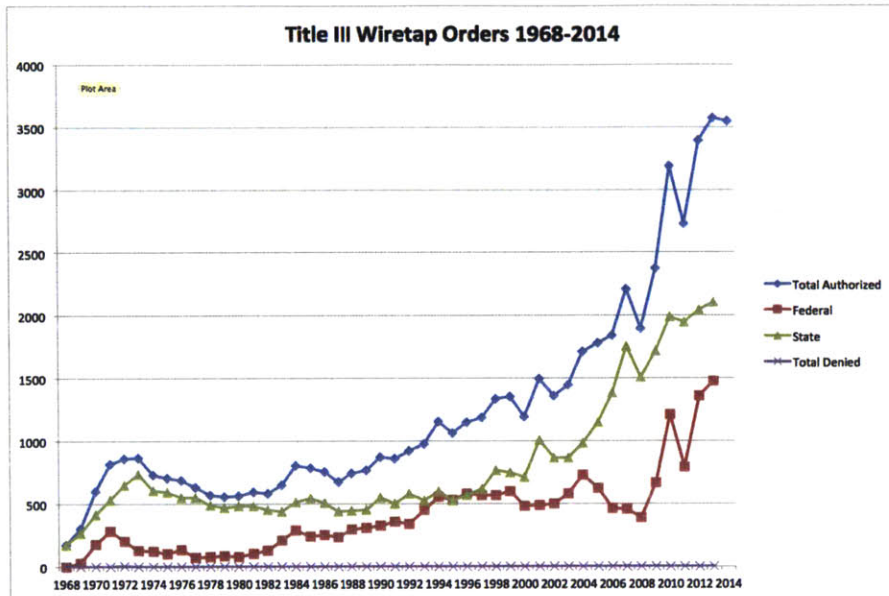


Figure 4. Graph on trends in wiretapping (Source: EPIC)

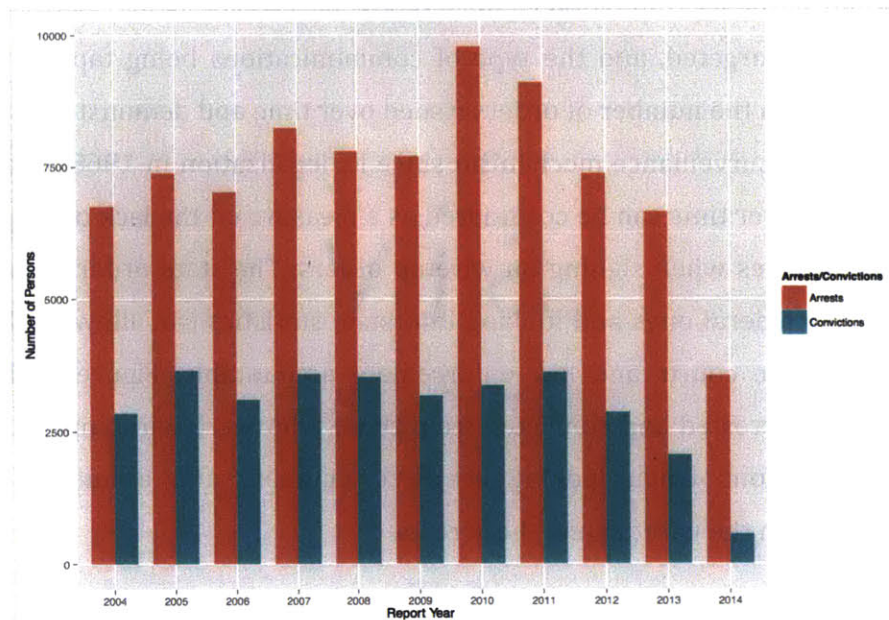


Figure 5. Trend of arrests and convictions related to wiretaps

The transparency is particularly beneficial when one begins to look at the granularity of prosecutors or judges. For example, Figure 6 shows a large number of cases from California in the 2014 Wiretap Report and digging into the data can reveal more about the jurisdiction and more targeted efforts towards accountability if trends spike over time. Looking within the California dataset can reveal the jurisdiction with the most wiretaps and the relevant crime and prosecutors issuing the orders. An analysis of the data shows that the majority of the wiretaps are for narcotics. Figure 7 shows the

California dataset categorized by the number of orders issued in each jurisdiction and clearly shows the most number of wiretaps being conducted in Riverside. A peek inside the data on Riverside can further reveal the prosecutors responsible. In this case, two prosecutors are identified in Riverside as Datig and Van Wagenen with the latter giving more than 450 orders and the former less than a 100.

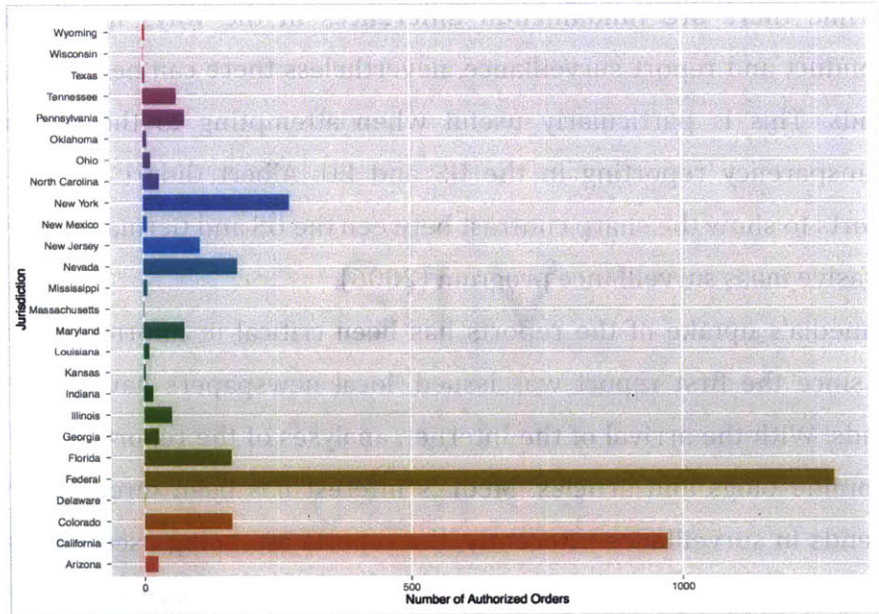


Figure 6. Number of Authorized Orders for Different States

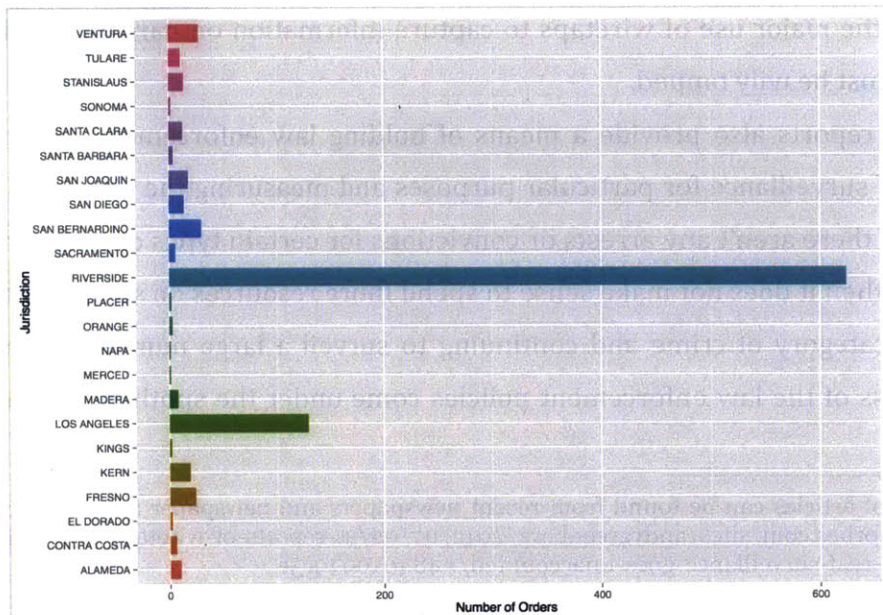


Figure 7. Number of Authorized Orders for California

The reports, in the past have been used to compare the levels of surveillance in the U.S. against those of other countries. For example, Paul M. Schwartz compared U.S. and

Germany in 2002 using the data available on both countries (2002). Schwartz drew on similarities such as the fact that investigations pertaining to narcotics lead to the highest percentage of surveillance orders, some geographic areas in both countries attracting a disproportionate amount of surveillance orders. In addition, relative population statistics showed German law enforcement agencies conducted more wiretaps. While there are fundamental differences in the ways in which different countries conduct and report surveillance, nevertheless there can be ways to compare certain trends. This is particularly useful when attempting to bridge the gap between transparency reporting in the US and EU. Albert Gidari Jr., also used the wiretap reports to show the sharp contrast between the US and Germany in terms of the latter's pervasive mass surveillance program (2006).

The media's uptake of the reports has been critical in informing the public at large. Ever since the first report was issued, local newspapers have been reporting general trends. With the arrival of the Internet, analyses of the reports made their way to various online blogs and articles. Media's interest has been directed towards the changing trends in surveillance.³ Recently, the reports are being used by the media to predict increased surveillance online as more corporate transparency reports surface. The type of offenses investigated in the wiretap reports has also drawn attention. In particular, the major use of wiretaps to capture information on narcotic dealings⁴, and the areas most heavily tapped.

The reports also provide a means of holding law enforcement accountable on their use of surveillance for particular purposes and measuring the effectiveness of the wiretaps. If there aren't any arrests or convictions for certain types of crimes as a result of the taps then it does not make sense to spend more resources on surveillance for that particular category of crime and continuing to surveil a large number of people. The effectiveness of the law enforcement policies come under the spotlight and may result

³ A number of articles can be found from recent newspapers and newspaper archives. For example: <http://www.forbes.com/sites/andygreenberg/2012/07/02/as-reports-of-wiretaps-drop-the-governments-real-surveillance-goes-unaccounted/#484010949c5e>

Another report from 1983: "REPORT SAYS FEDERAL WIRETAPS ROSE 23% IN '82." The New York Times. (May 1, 1983 , Sunday, Late City Final Edition): 738 words. LexisNexis Academic. Web. Date Accessed: 2016/01/29.

⁴ An example of an article reporting on the use of wiretaps for narcotics: <http://motherboard.vice.com/read/almost-90-percent-of-all-us-wiretaps-listen-for-suspected-drug-deals>

in the public and civil society to impose pressure on the agencies. The wiretap report has been utilized by several organizations over the years that help provide statistics while advocating for surveillance reform.

While the overall number of wiretap orders issued may have gone down in 2014, the number of people intercepted went up. The number of arrests and convictions may need to be taken in with a grain of salt since there is a strong incentive to regard arrests as directly caused by evidence obtained from the wiretaps. Given the large number of people being intercepted and the low levels of “success”, policies may need to be reconsidered. In order to make a more informed judgment, data for the next few years will continue to be relevant as more arrests and convictions may take place as a result of the wiretaps conducted in these periods. The statistics on arrests and convictions are misleading since the wiretap itself might not have been relevant in arresting someone or convicting them. This may give a false picture of the effectiveness of the surveillance technique and may result in law enforcement exaggerating the necessity of wiretaps. Herman Schwartz, in 1972 uncovered several results that undercut claims of the usefulness of wiretap reports. (Diffie & Landau, 2007) In *United States versus Poeta*, the US Court of Appeals observed that the tap related evidence was irrelevant to the conviction, and in *Uniformed Sanitation Men versus Commission of Sanitation*, the court made the same observation (Schwartz, 1974 cited in Diffie & Landau, 2007). Schwartz also found that law enforcement personnel were predisposed to exaggerating the number of incriminating evidence in their reports e.g. in *United States versus King*, the government claimed that 80-85% of the tapped conversations in a drug case were incriminating while the Court felt they were between 5 and 25% (Schwartz, 1974 cited in Diffie & Landau, 2007). Table 2 contains numbers on the arrests and convictions said to have been related to the wiretaps between 2012 and 2014.

Many of the prosecutor reports for the federal wiretaps are missing and they may enter the next few reports. Figures 8 and 9 show the proportion of prosecutor reports missing from the dataset of reports between 2012 and 2014. The reports have been criticized for underreporting as indicated by the mismatch between the number of reports from the state courts and prosecutors (Kennedy & Swire, 2002). In the 2014 Wiretap Report, a prosecutor did not report on 1040 orders out of a total of 2181 approved by the District Court. In addition, 130 out of 2628 orders approved by the State Courts were also not addressed via prosecutor reports. The absence of prosecutor

reports also results in a lack of information on the number of arrests, incriminating evidence, average number of intercepts among other pieces of relevant information. But the onus of the blame lies upon the prosecutors and not the AO since the latter’s job is only to collect, organize and convey the reports. Currently the explanation provided by the AO for missing prosecutor reports on certain orders is that either the report was submitted too late for it to have entered the dataset for the year or that prosecutors purposefully choose not to, to avoid endangering ongoing investigations (US Courts, 2014). However, another reason may be that the prosecuting officials have not been reporting accurately due to a lack of incentive resulting from zero congressional oversight in years.

Year	Number of People Intercepted (n)	Arrests (a)		Convictions	
		Number	As % of n	Number	As % of a
2012	381545	3074	~0.35%	556	~18.09%
2013	165211	3240	~1.96%	682	~21.05%
2014	165420	2317	~1.4%	410	~17.69%

Table 2

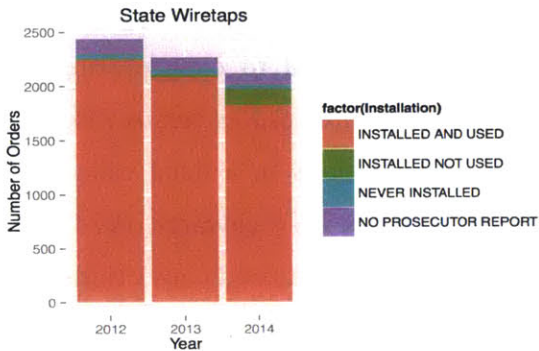


Figure 8.

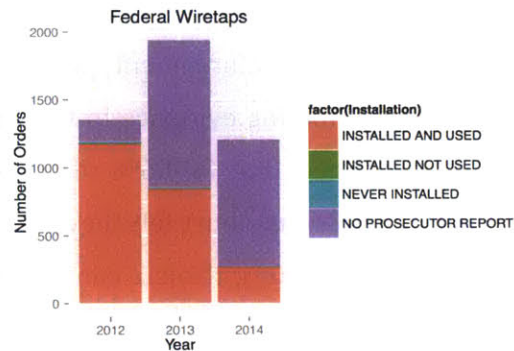


Figure 9.

Using the wiretap statistics, Diffie and Landau debunked former FBI Director Louis Freeh’s claim that new communications technologies were hindering the FBI from solving several cases, including those involving kidnapping. The statistics at the time revealed that only an average of 2-3 wiretaps were used for kidnapping cases while the annual number of kidnappings was usually close to 450 (Diffie & Landau, 2007).

The Electronic Privacy Information Center (EPIC) is a non-profit public interest research group routinely files amicus briefs in federal courts, pursues open government cases and speaks before Congress and judicial organizations regarding evolving privacy and civil liberties issues. EPIC has been publishing graphs and statistics based on the wiretap reports dating all the way back to 1968⁵. EPIC releases statistics representing the trend of ongoing surveillance based on the reports. These trends typically cover the number of orders issues, the types of crimes being targeted and limitations imposed by encryption for law enforcement agencies. The center has also cited the reports in letters to the government for better accountability and transparency for other surveillance mechanisms including “pen register” and “trap and trace” surveillance. Overall, EPIC has been a key provider of information to the public regarding the reports and significant changes in trends. An Amicus Curiae represented by EPIC in support of removal of gag orders on NSLs also recognized the importance of the wiretap statistics.

A recent report (Balkovich et al., 2015) by RAND Corporation on mobile surveillance compares wiretapping reports with the Google Transparency Reports to show the changing face of surveillance:

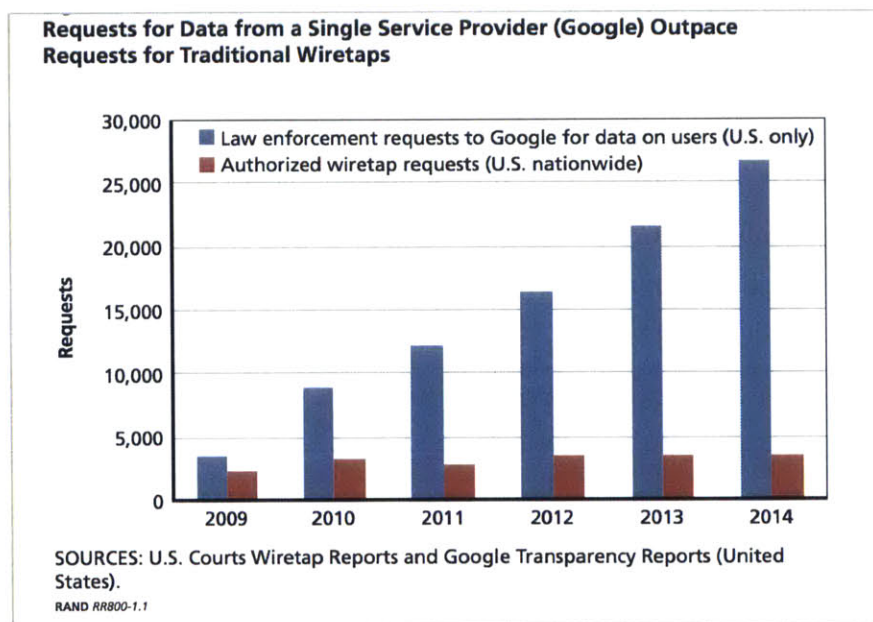


Figure 10.

The ACLU has cited wiretap statistics on multiple occasions to challenge proposals mandating weaker encryption for e.g., in a written statement before the US

⁵ EPIC maintains its repository of statistics at the following URL: https://epic.org/privacy/wiretap/stats/wiretap_stats.html

House Committee on the Judiciary Subcommittee on Crime, Terrorism and Homeland Security against the proposed updates to CALEA⁶.

The Electronic Frontier Foundation (EFF) has used the reports on multiple occasions to challenge the enforcement of laws mandating services to remain “wiretap friendly” through CALEA (Slater, 2006). EFF has also drawn attention of the public to the status of surveillance programs by providing trends to demonstrate more people and conversations not linked to criminal activities being recorded (Fakhoury, 2012).

Pew Research Center conducted an analysis of the report using the metric number of wiretaps per 500,000 people (Shelton, 2014). Nevada topped the list and while the reason has not been identified, there is some speculation that it might have to do something with the high statistics of crime in the region.

The statistics have also played a key part in the long-standing debate on encryption, backdoors and forced vulnerabilities in telecommunication devices. The statistics showed scarce instances of law enforcement agencies being inhibited by encryption and unable to access the required data. As Diffie and Landau put it: “encryption in wiretapped communications is simply not a problem for law enforcement” (2007). The failure of law enforcement agencies to provide specific numbers on the surveillance thwarted by encryption has led to civil liberties groups looking into wiretap statistics to show that the problem has been overstated (Fenton, 2015). The first instance of encryption preventing access to communications was reported in the 2012 Wiretap Report. The following table (Table 3) provides details on encryption statistics from recent reports:

Report	Encountered	Access Prevented
2014	30*	8
2013	93**	61
2012	29***	4

Table 3

** 5 of these wiretaps are from previous years with 4 preventing access*

*** 52 of these are from previous years with all 52 instances preventing access*

**** 7 of these are from previous years.*

⁶ For example, see:

https://www.aclu.org/files/assets/ACLU_Statement_for_the_Record_On_Proposed_Updates_to_the_Communications_Assistance_to_Law_Enforcement_Act_CALEA.pdf

Others have used the encryption statistics to show how encryption is likely to affect surveillance while proposing the use of the Fifth Amendment's clause for compelled disclosure to be considered (Terzian, 2013). Recently, there have been efforts by companies such as Apple and Whatsapp to encrypt their services without holding any encryption keys themselves and this may lead to a change in the encryption statistics in future reports. When law enforcement agencies now approach these companies with warrants or court orders, the latter can no longer provide access to the encrypted data. However, there is always a danger that the encryption will become politicized if something were to go wrong and the law enforcement were to blame encryption for preventing law enforcement from acting in advance (Naughton, 2016). A recent report by the Harvard Berkman Center, however, argues that law enforcement will not be "going dark" soon due to a number of factors preventing the widespread use of end to end encryption (Berkman Centre for Internet and Society, 2016).

Limitations of the Wiretap Report

While the Report can be used as a powerful analytical tool to assess the value of the wiretaps over the decades, it has severe limitations. (Diffie & Landau, 2007) The Report has been criticized for being inaccurate, misleading and providing an incomplete view of surveillance mechanisms employed by the state.

The first line of arguments that is often hurled against the utility of the reports is that they cover very little ground of the surveillance landscape. David Sullivan, Policy & Communications Director at the Global Network Initiative (GNI) argues that the reports only cover a small percentage of the total surveillance being done and greater transparency is needed (2013). This has been widely echoed by different researchers as well as media outlets.

Recently, the discrepancy between the number of orders in the Wiretap Report and the numbers provided by telecom companies has cast a shadow of doubt on the accuracy of current and past reports. In 2012, Congressman Ed Markey released a collection of letters he received from major phone after he demanded they reveal how often they disclose users' data to the government and under what circumstances. Some of the responses received from the companies show the inaccuracy of the official wiretap reports as the numbers pale in comparison to the numbers reported by the

companies (Greenberg, 2012). Transparency reports by Verizon, AT&T, Sprint and T-Mobile in 2014 reported wiretap figures that are three times the number of wiretaps reported in the 2014 AO report. (Gidari, 2015). As detailed as the Wiretap Report is, it lacks one key piece of information: the names of the telecommunications carriers that received and complied with the intercept orders.

The reports have also been criticized for being “misleading” as single orders for wiretaps can affect hundreds of lines (Froomkin, 2010). For example, the total number of wiretaps in the 2014 Wiretap Report is 4809 but the total number of individuals intercepted was 643537⁷. These numbers include continuing orders from previous years that were previously unreported and are hence, different from the numbers in the graphs above. While the media is usually quick to capture the trends in the number of orders, it usually fails to look at the number of people affected. The number of orders appears to be un-alarmingly small but the figure on the persons intercepted paints a dramatically different picture.

Conclusion

The Wiretap Report despite its weaknesses provides a window into the workings of the surveillance state and an opportunity for discussions on surveillance to be made in the public sphere. The numbers have been some of the very few statistics available on surveillance for several decades and were often used to measure changes in surveillance strategy by the media, academics and civil society. The rise of transparency reports provide a way of holding law enforcement and the courts accountable for accurate reporting and we can expect there to be an improvement in the accuracy of the Report in the future.

Given the elaborate list of details required for each wiretap order, the Report provides us with a “gold standard” to compare the levels of transparency for other forms of surveillance. Establishing the Report as a model helps pave the direction the corporate transparency reports and government issued reports need to take in order to bridge the surveillance-transparency gap and improve accountability.

⁷ These numbers are based on both state and federal wiretap statistics.

Chapter III

Transparency Reports

There is now business value in championing privacy and fighting the NSA, and business harm in cooperation. There are basically four means by which corporations can fight: transparency, technology, litigation and lobbying.

- Bruce Schneier

As companies scrambled to rectify their public image in the aftermath of the Snowden disclosures, one particular tool that rose in popularity was the *transparency report*. The report provided a way forward for ICT companies to become more transparent about their data sharing practices with the government. This chapter takes a closer look at the transparency reporting practices by companies and demonstrates the challenges that prevent the reports from becoming useful tools for stakeholders. The chapter also introduces a model transparency report that takes into account the prevailing best practices and additional features that should be present in the report.

Before the Snowden leaks, only a handful of companies published transparency reports and the number of companies publishing reports skyrocketed in the aftermath of the leaks. The first well-known Transparency Report was published by Google in 2010 in an attempt to convince privacy and transparency advocates that it was on their side (Miller, 2010). Google published its report with the goal of initiating a conversation about censorship and surveillance, motivated by its commitments as a member of the GNI (MacKinnon, 2011). The report contained a map showing takedown requests by governments and requests for user data along with the percentage of requests Google complied with. Since then, the report has evolved and the current format⁸ contains several categories ranging from content removal to encryption of email in transit. The current report provides the number of requests by each country, the number of user accounts affected and the percentage of requests Google complied with. The report also features a breakdown of requests based on the legal framework that is used to request them i.e. subpoena, warrant, emergency disclosure, Wiretap Order, Pen Register Order, and “other” requests.

⁸ The Google Transparency Report can be accessed at google.com/transparency

Contrary to popular belief, Google's report was not the first attempt by the ICT industry to report statistics on government surveillance. Transparency reports were first experimented with in the 2000's with *rsync.net* maintaining one since about 2006 and featuring a warrant canary⁹ (Knox, 2015). According to Chris Soghoian, AOL was the first company to disclose statistics on government requests in 2006 by revealing to the New York Times that it received 1000 requests per month (2010). Then in 2007, Verizon responded to queries from various members of Congress to announce that it received requests averaging 90,000 per year from government agencies (Soghoian, 2010). So the concept of reporting statistics on government requests for user data was not necessarily novel but the format and mode of presenting the report, as Google did, was unique.

The reports have now become a norm in the ICT industry and companies regard publishing them as an example of good governance and a road map for the development of corporate ethics for companies dealing with user data (Kulikova, 2013). The format and level of detail published in a transparency report varies across the industry and companies pick their own format and representation. It is, however, fair to say that Google's report may have had some level of influence on companies that were new to publishing such reports. The graph¹⁰ in Figure 1 shows the growth in transparency reporting over the years since 2010 with the first report in 2010 belonging to Google.

Transparency reports come in different formats, shapes and sizes with varying level of detail. Google's Transparency Report features static tables and charts that describe the different statistics related to requests. Twitter's transparency report (Twitter, 2015) features an interactive map that dynamically responds to the cursor position on the world map and displays bar and pie charts corresponding to those regions. Zooming in on the U.S. provides statistics on requests at the state level. Microsoft's *Law Enforcement Requests Report* (Microsoft, 2015) is a blend of Google and Twitter's reports and features a map and charts featuring the statistics. Most reports include qualitative data in the form of explanations of company policies regarding the requests, what the numbers mean, limitations of the data and FAQs. Some companies

⁹ The warrant Canary can be seen on the following URL: <http://www.rsync.net/resources/notices/canary.txt> (Accessed 20th March 2016)

¹⁰ This graph is based on data from the Access Now Transparency Reporting Index (Access Now, 2016) which provides the initial date of release for each transparency report.

also allow the data to be downloaded in a .csv format, thereby, facilitating analysis. **Appendix A** contains a few snapshots of transparency reports published by different companies.

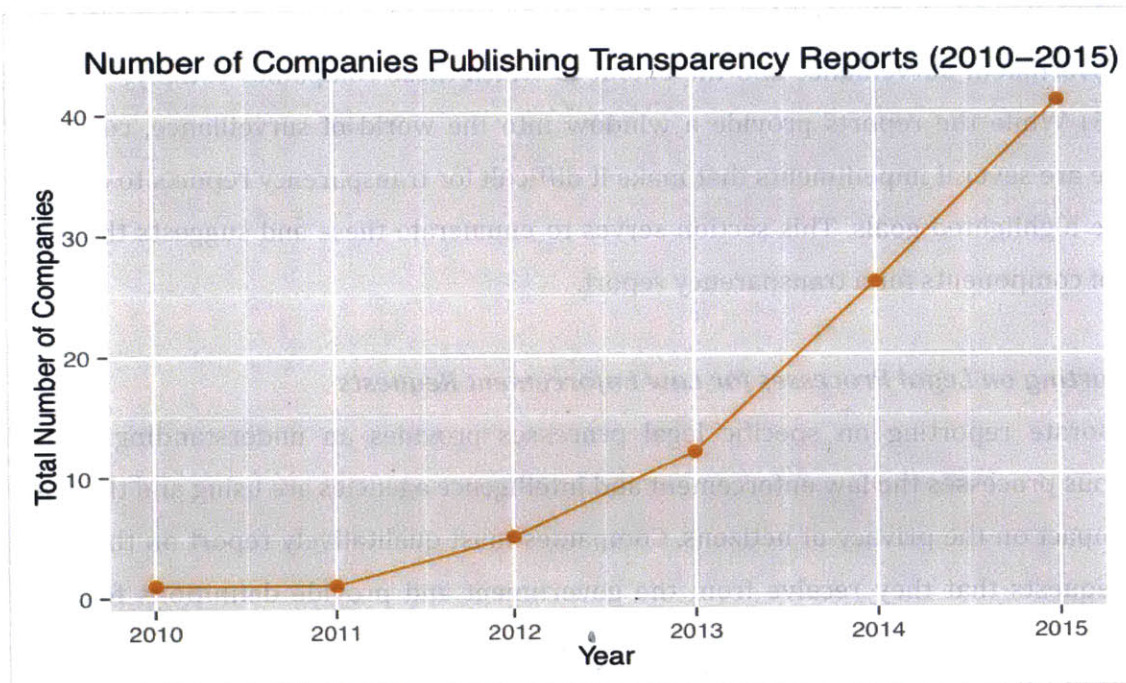


Figure 1. This figure shows the rise in the number of US companies publishing transparency reports.

Other than statistics and supplementary explanations, some companies also publish, “warrant canaries”. Canaries are essentially statements by companies that they have not received a request from a particular legal process e.g. subpoenas, NSLs etc. A removal of the statement indicates that the company has received such a request and that it is barred from stating that it has received it. Apple’s first transparency report featured a canary claiming that it had “never received an order under Section 215 of the USA Patriot Act” (Apple, 2013). The canary disappeared afterwards with experts drawing different conclusions as to the reasons for its removal (Roberts, 2014).

Evaluating The Usefulness of Transparency Reports

At the onset, the reports provide much needed transparency in a landscape historically shrouded by secrecy. In order to be useful as policy tools, the reports need to fulfill two broad goals. First, the reports should be able provide an overall picture of surveillance and the practical interpretation of surveillance statutes by the government and law enforcement authorities. Second, they should serve as a way to compare the

performance of different companies across the industry and over time. Being able to aggregate statistics and observe trends would assist civil society and activists to impose greater pressure on the government for surveillance reform if necessary. In addition, would help stakeholders understand the pressures placed on companies to participate in government surveillance and the extent to which these companies comply.” (Losey, 2015) While the reports provide a window into the world of surveillance, currently there are several impediments that make it difficult for transparency reports to achieve these highlighted goals. This section serves to enumerate these and suggests the ideal set of components for a transparency report.

Reporting on Legal Processes for Law Enforcement Requests

Corporate reporting on specific legal processes provides an understanding of the various processes the law enforcement and intelligence agencies are using and the scale of impact on the privacy of netizens. Companies must qualitatively report on the types of requests that they receive from the government and provide definitions for each process and the type of data they hand over as a result of having received a request for each. This is particularly important as it determines how the government is interpreting law into practice in determining what kind of data it is requiring from the company. For example, in traditional terms, wiretap and pen register / trap and trace orders were primarily for telephonic conversations and it would be useful to know how they translate to online services. In addition, companies must provide information on the numbers of requests they receive for each legal process, the number of users¹¹ specified in those requests, company’s rate of compliance and the number of users impacted as a result. While all these features are desired from transparency reports, there is a wide variation in terms of the granularity companies report in and this impeded any industry-wide aggregate or comparative analysis. A complete list of legal authorities that are used to demand data from companies is given in Table 1.

¹¹ The term “users” may be different depending on the context and the type of business. E.g. Apple’s report mentions the number of *devices* specified rather than users. Similarly, Tumblr’s report mentions the number of *blogs* affected.

Process	Statute	Type of Data
Subpoena	Stored Communications Act	Stored, non-content
Search Warrant	Stored Communications Act	Stored, content and Non-Content
Other Court Orders (D Order)	Stored Communications Act	Stored, Non-Content
Wiretap Order	Wiretap Act	Real Time, Content
Pen Register / Trap and Trace	Pen Register Act	Real Time, Non-Content
Emergency Disclosures	Stored Communications Act	Stored, Content and Non-content
National Security Letter	18 U.S.C. §2709	Stored, non-content
FISA Order	50 U.S.C. §1804	Stored/Real Time, Content and Non-Content

Table 1.

	Stored Communications Act	Wiretap Act	Pen Register Statute
Content	"[Any] record or other information pertaining to a subscriber or customer of such service (not including the contents of communications)," including basic subscriber information such as "any information concerning the substance, purport, or meaning of [any wire, oral, or electronic] communication"		N/A
Non-Content	"name; address; local and long distance telephone connection records, or records of session times and durations; length of service ... and types of service utilized; telephone or instrument number or other subscriber number or identity ... and means and source of payment for such service (including any credit card or bank account number)."	N/A	"dialing, routing, addressing, or signaling information ... not includ[ing] the contents of any communication"

Table 2. Taken from the Transparency Reporting Toolkit (Woolery et al., 2016) shows the type of information for content and non-content data under the law enforcement statutes providing access to data.

Reporting at the level of process granularity also helps hold the government accountable for the types of processes that it publishes its own transparency reports for. The number of wiretap orders may be used to provide a layer of accountability to company reporting practices but this might not be successful unless all companies begin to publish at the level of granularity featuring different legal processes. Reports by companies can also help hold the courts accountable for incorrect reporting. Even without a comprehensive number of wiretap orders reported by companies, current data reveals an alarming result when compared against the official statistics published

under the Wiretap Report. The following graph (Figure 2) was generated using the number of Wiretap orders published by companies for the year 2014 and the number of wiretap orders authorized by the US State and Federal Courts in 2014¹²:

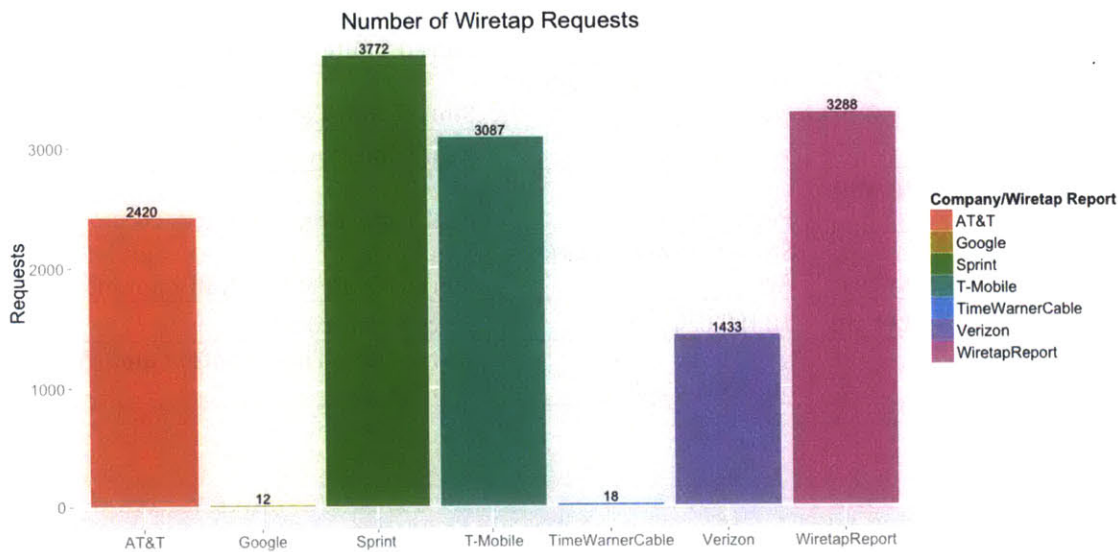


Figure 2. The figure shows the number of wiretaps received by 6 companies as indicated in their transparency reports for 2014 and the number of and the state and federal wiretaps reported in the 2014 Wiretap Report in the right-most bar.

The graph shows that the wiretap requests received by a single company - Sprint outstripped the total number of wiretaps issued by the AO in the Wiretap Report for 2014. The total number of wiretaps reported by these companies completely shadow the number reported in the official Wiretap Report. This may point towards incorrect reporting, incorrect internal company definitions for what counts as a wiretap order, or wiretaps being conducted without court approval. In either of these cases, the example shows the potential power of the reports in holding the government accountable and in adding value to debates on greater transparency and surveillance reform. More companies reporting such statistics over time can continue to hold the authorities accountable and this might improve the official reporting processes as well.

Most companies do not report at the same level of granularity of legal processes and tend to group certain requests together under an overarching term such as “law

¹² The graph is based on the transparency reports for the companies identified in the graph and the Wiretap Report for 2014 uploaded on the U.S. Courts website. The graph excludes the number of supplementary wiretaps reported in the 2014 Wiretap Report by the AO and the number of wiretaps that were authorized but never installed.

enforcement requests”¹³. The Transparency Reporting Toolkit identifies the prevailing best practice of reporting on individual legal processes as individually reporting on the following processes: search warrants, subpoenas, other court orders (e.g., 18 U.S.C. § 2703(d) orders), wiretap orders, pen register orders, and emergency requests. (2016) Google, for example reports on each type of order while Apple and Microsoft clump all law enforcement requests together and report them as a single number.

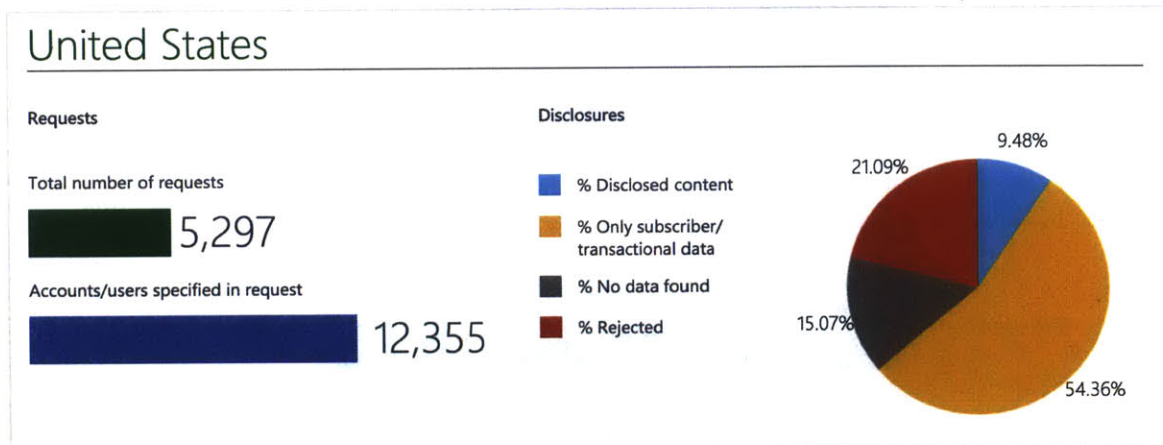


Figure 3. Screenshot of Microsoft’s 2015 Law Enforcement Requests Report with no granularity

Detailed Data

The table below provides the number of government requests for user data from the United States issued by U.S. authorities for U.S. criminal investigations as well as requests made on behalf of other governments pursuant to mutual legal assistance treaties and other diplomatic mechanisms. For more information, please refer to our FAQ about legal process.

Reporting Period	User Data Requests	Users/Accounts	Percentage of requests where some data produced
January to June 2015	12,002	31,343	78%
Subpoena	7,032	21,667	74%
Search Warrant	3,588	6,730	85%
Other Court Orders	929	2,310	78%
Emergency Disclosure Requests	236	351	69%
Pen Register Order	212	279	88%
Wiretap Order	5	6	100%
Preservation Requests	5,052	11,985	—

Figure 4. Screenshot of Google’s Transparency Report for the US in 2015

In terms of the quality of definitions provided for each legal process, the Transparency Reporting Toolkit identifies only two companies (Google and Verizon) demonstrating the best practice of “clear and comprehensive explanations of legal process” in their reports (Woolery et al., 2016). A summary of the numbers of

¹³ This is a term used in Microsoft’s Transparency Report.

companies reporting on different processes can be seen in Figure 5. The definitions are particularly important in informing the general public that might not be aware of the legal mechanisms in place for requiring data from companies.

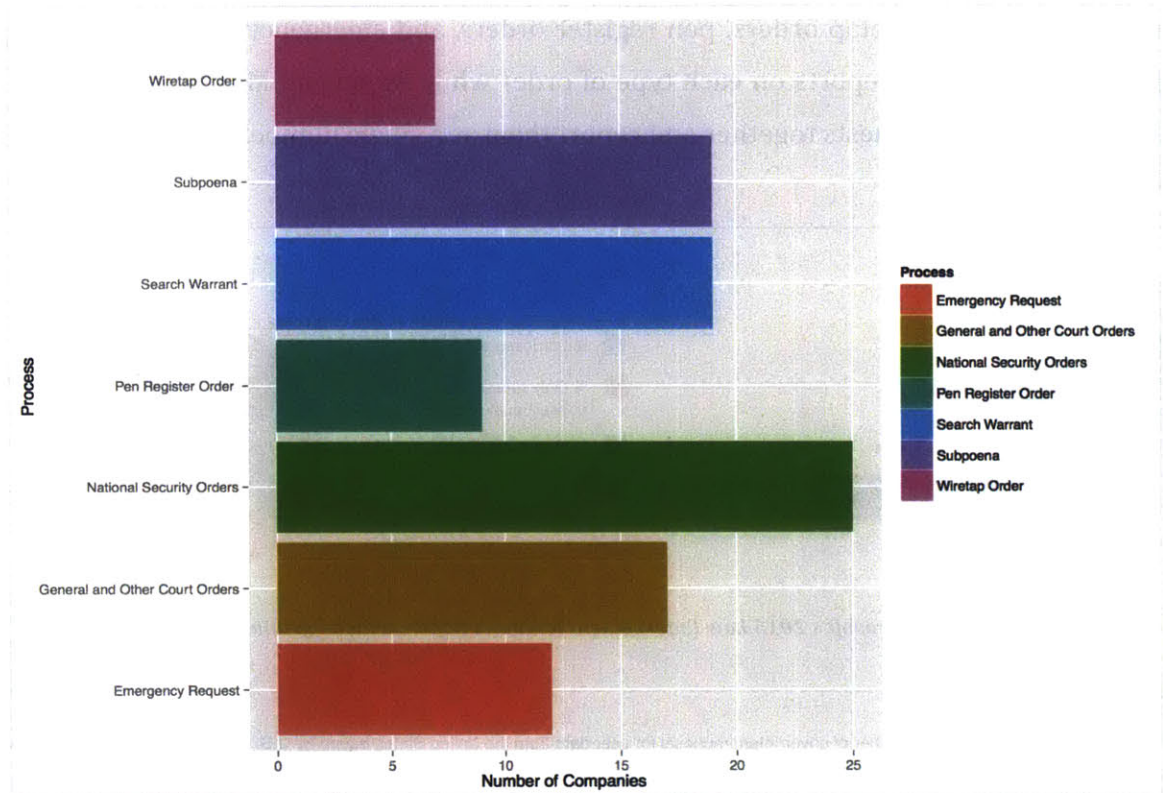


Figure 5. Legal processes individually reported by companies¹⁴

There is a lack of standardization across the industry in terms of the terminology and definitions used to describe the different processes and this may impede automated analysis of reports. Manually, it may be easy to determine the similarity or difference between terminologies e.g. “search warrant” vs. “warrants” or “emergency requests” vs. “emergency disclosures”, however, it may not be as easy for code for all possible variations. With the number of reports increasing every year, any attempt to gather and aggregate all data in the presence of varying terminology will result in large resource costs, impeding aggregation and subsequent analysis.

There is also the need for companies to provide qualitative information on the types of data they disclose under each legal process and quantitative data on the types of data being requested by the government under each order in the form of numbers or percentages. Google provides some transparency in this regard but does not provide a

¹⁴ This graph was plotted using data from the Transparency Reporting Toolkit in addition to taking into account Uber’s Transparency Report launched in April 2016.

detailed list of data that can be acquired under each process. For example, Google in its definitions for the various legal processes provides some information on what each process can compel Google to disclose. **Table 1** shows the type of data Google can reveal for Gmail under different legal authorities (Google, 2015). Figure ___ shows the type of data released for YouTube under different legal processes.

Subpoena	<ul style="list-style-type: none"> Subscriber registration information (e.g., name, account creation information, associated email addresses, phone number) Sign-in IP addresses and associated time stamps
Search Warrant	<ul style="list-style-type: none"> Email content Information obtainable with a subpoena or court order
Court Order	<ul style="list-style-type: none"> Non-content information (such as non-content email header information) Information obtainable with a subpoena
Emergency Disclosures	<p>"Sometimes we voluntarily disclose user information to government agencies when we believe that doing so is necessary to prevent death or serious physical harm to someone. The law allows us to make these exceptions, such as in cases involving kidnapping or bomb threats."</p>

Table 3

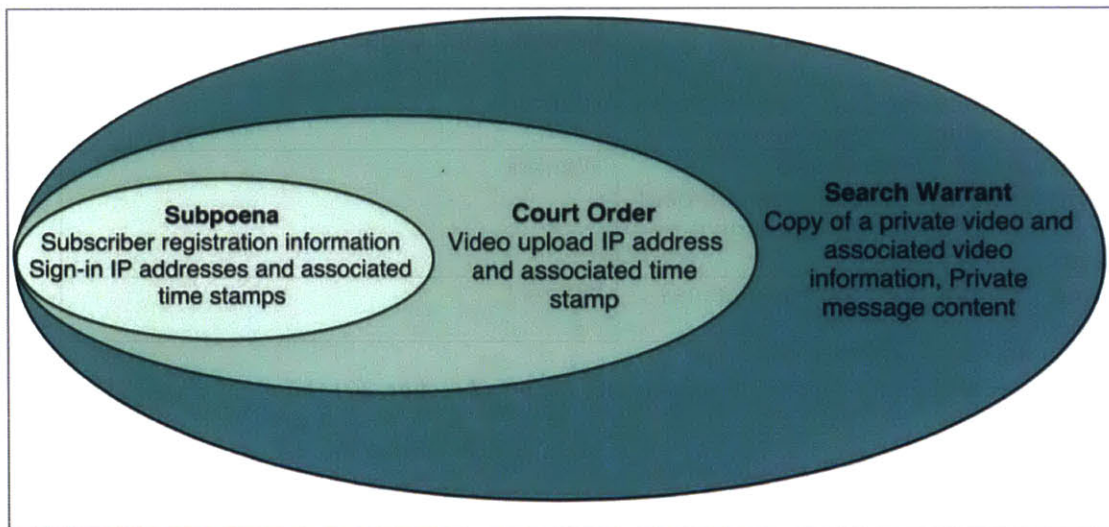


Figure 6. The figure shows the type of data that Google hands over for YouTube when faced with different requests. It has been create using publicly available information provided by Google in on its transparency website.

OTI and Berkman Center’s Transparency Reporting Toolkit has identified T-Mobile’s report as providing the best practice of detailed accounting of legal process required by the company to turn over specific types of user information (2016). Table 3 and Figure 6 provide somewhat clear understanding of what legal process is required by

companies to disclose certain information. Compared to Google’s explanation of potential types of data under each process, T-Mobile’s report provides a more detailed outline (Table 4).

Information Type Requested	Minimum Required Legal Process
Subscriber Information (e.g., information a customer provides when signing up for service, such as name and address, and call detail information)	Subpoena
Historical Call Detail Information (e.g., information about calls made in the past, such as start time, duration, numbers called)	Subpoena
Emergency Information (e.g., location information, call detail, content, in emergencies)	Certification from Law Enforcement/Public Safety Answering Points
Real Time Call Detail Information (e.g., information on incoming and outgoing phone numbers for a specific phone/mobile device)	Pen Register Court Order
Historical Cell Site Location Information (e.g., location of towers that a phone/mobile device used in the past over a specific period of time)	Court Order or Warrant*
Real Time Audio (e.g., phone conversation)	Wiretap Court Order
Real Time Content (e.g., text messages)	Wiretap Court Order
Real Time Location (e.g., approximate location of a phone/mobile device)	Warrant
Historical Cell Tower Dump Information (e.g., list of phone numbers which used a specific tower during a specific period of time)	Warrant
Stored Content (e.g., saved voicemail message)	Warrant

* Depends on the applicable jurisdiction.

Table 4: Screenshot from T-Mobile’s Transparency Report (T-Mobile, 2014)

Reporting on Emergency Disclosures

Emergency requests and disclosures are an area of concern for users and stakeholders as this authority may be abused and could be a potential loophole for authorities wishing to gather data without court approval. Therefore, it should be expected of companies to report on the type of requests that they are receiving for emergency requests based on a number of categories e.g. kidnapping, gambling, etc. This form of reporting however, may be subject to non-disclosures in certain events and companies may need to be cognizant of this while reporting.

In addition to reporting on the type of crime, companies must also report on the type of data disclosed in emergency situations. For example, T-Mobile provides a few examples of the type of data it might disclose: location information, call detail, and content. Since emergency disclosures occur in the absence of a court authorized request, there needs to be transparency regarding the types of data that can be handed.

Reporting on Levels of Compliance

Reporting on the number or percentage of requests that companies have complied with for each type of request is essential to determining company practices over time. In order to conduct a more scrupulous analysis of compliance over time, there is also a need for companies to report on reasons for non-compliance and perhaps grouping them into different categories e.g. incorrect legal authority, request was too broad, no data was found etc.

Many companies provide numbers on the requests they complied with. In terms of accountability, it is difficult to know how real the numbers are as there is an incentive to fabricate results to indicate lower compliance over time. Even if the numbers are to be trusted, compliance rate statistics are misleading as they give an impression that some companies might be better at guarding data than others whereas it might not be the case. What is needed is information on why companies reject certain requests in order to be able to compare the vetting behavior of different companies when faced with requests for user data.

Reporting on Users Impacted

Ideally, we would like to see companies reporting on the number of users specified in legal requests and the number of individuals impacted as a result of the company complying with the request. The Transparency Reporting Toolkit identifies the following best practices (2016):

1. Report the number of selectors specified in a request
2. Report the number of users and/or accounts responsive to a request

Only Google, Snapchat and Verizon are deemed as being close to the best standard according to the report. Several companies do not report both types of information. One request may affect multiple user accounts and so the metric indicating the number of requests is misleading as it hides the actual scale of the number of individuals affected.

The Wiretap Report for instance, shows how a single order can affect many individuals. This phenomenon is also captured in Dropbox's Transparency Report (Dropbox, 2015). The Report points out that for each piece legal process: "Some may identify a single account, whereas others identify tens of accounts in a single request". (2015) Dropbox however, only reports on the numbers of accounts specified in the request and does not provide any numbers on the accounts affected as a result of complying with the request.

Location Statistics

As far as location granularity is concerned, we would like to see companies reporting numbers for each US state and for each country for international requests. Twitter, Tumblr and Credo Mobile have been providing numbers of requests made by authorities in each U.S. state. Credo Mobile goes a bit further and also reports the state the customer resides in (Credo Mobile, 2015). Trends over time can help civil society and citizens hold their state officials to account. For example, Twitter's reports show a sharp increase in the number of requests within a year. If other companies made such data available, similar trends could help stakeholders exert greater pressure on state authorities and in keeping a check on their surveillance activities. This may lead to justifications offered by state official, which may then be evaluated via debate in the public sphere on balancing personal liberties and the welfare of the state. Data can tell stories. A number of correlations may be drawn between events in certain states and the levels of surveillance. While it is difficult to prove correlation using the small dataset available from Twitter, aggregated industry wide numbers may help point towards state law enforcement activities resulting in a more targeted effort towards state surveillance reform. Perhaps increase in requests within certain states might be correlated with ongoing events e.g. the #blacklivesmatter movement and potential abuse of surveillance powers may be caught through aggregated industry wide, state specific data on requests. The graph¹⁵ in Figure 7 shows the top five states with the most number of reports, showing a sharp spike in requests from California, New York and Virginia. Currently, only Twitter and Tumblr are the only two companies that report on the number of requests made by each state. On discussing this type of reporting with Ryan

¹⁵ This graph was created using the number of requests in the Twitter Transparency Report on the U.S.
<https://transparency.twitter.com/information-requests/>

Budish, he was unsure whether this should be considered the “best standard” and if companies would be willing to report to such a degree.

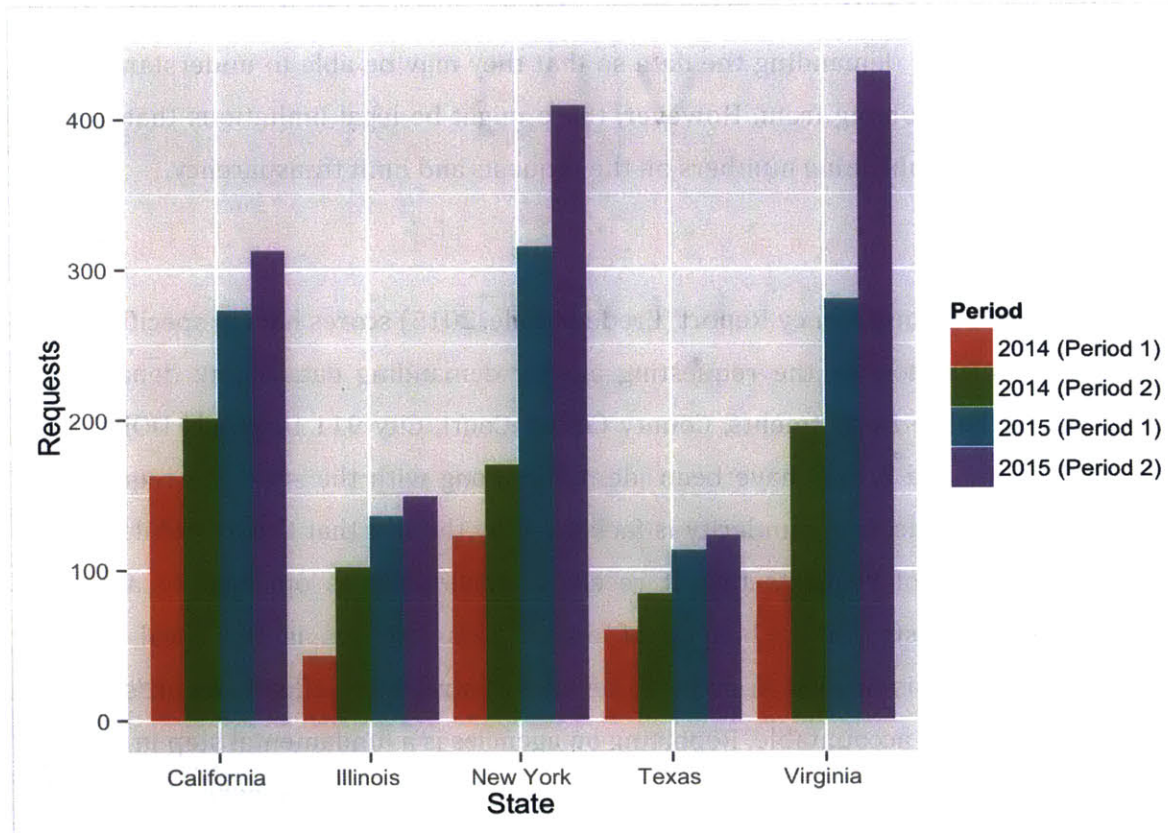


Figure 7. Top 5 US states with the most requests in Twitter's Transparency Reports

Reporting on international requests is important to ensure that U.S. companies do not become complicit in invading the privacy of users under strict or authoritarian regimes where restrictions on speech may result in dire consequences such as arrests or heavy penalties. For example, a new bill in Pakistan, the *Prevention of Electronic Crimes Act* seeks to impose heavy penalties and long sentences on citizens who criticize the civilian government on social media. Any attempts by the Government to seek information on the location of content of such users must be blocked. Facebook currently has the highest rate of compliance when responding to requests from Pakistan (58.33%) in the first half of 2015. If the bill is passed in the Senate, the compliance from Facebook should ideally fall. While reporting on international requests is not central to this thesis, it is important to realize that there is the need for data at the granularity of each country. A category of statistics that often go unreported are the legal processes being used to demand data from different countries. A comparison of reports published by

Facebook, Google, LinkedIn, Microsoft, Tumblr, Twitter, Verizon, and Yahoo, reveals that none of these companies reported legal processes used for request for users data from non-U.S. governments (Losey, 2015). These statistics can be important for civil activists from the countries demanding the data so that they may be able to understand where the requests are coming from. However, there might be legal limitations that prevent companies from publishing numbers on the requests and limit transparency.

Agency Reporting

Credo Mobile's Transparency Report (Credo Mobile, 2015) scores high in specificity as it provides information on the requesting agency demanding data. Many departments such as City Police Departments, County Circuit Court, City 911 Dispatch, DOJ, County Sheriff's Office and others have been identified along with the state the request was made in. This particular granularity is facilitated by the fact that Credo Mobile reports the few number of requests that it receives individually as opposed to aggregate number of requests for each type of order. This perhaps is the ideal level of transparency that is needed in order to be able to streamline efforts towards holding certain authorities accountable. Reporting on agencies is a fundamental step in the right direction and may have the potential to catch abuses of power. While it is understandable that this may be difficult for companies receiving thousands of requests to publish at the granularity of each request and the corresponding agency making the request, perhaps they may consider reporting in percentages the agencies making the most requests. Another strategy may be to report on agencies at the granularity of each US state.

Reporting on National Security Requests

Perfect transparency would entail that companies report the exact number of FISA orders and NSLs and the number of users affected but legal limitations on transparency through reporting restrictions and nondisclosure orders restrict the transparency of national security requests. Therefore, companies must report in bands defined under the USA Freedom Act (Table 5). The bands allow both requests and the number of user accounts affected to be reported. The survey in the Transparency Reporting Toolkit shows there is a variation in the choice of bands that companies choose to report in. The bands provide insufficient transparency on an aggregated industry level they cannot be

added up to provide an accurate picture of the scale of surveillance through the two types of orders. What companies can do more of is to report on the types of data they can disclose with each request and to provide ranges for the number of NSLs, content based FISA orders, non-content FISA orders and the customers targeted in each. Since the Freedom Act also allows companies to challenge non-disclosure orders, perhaps numbers of orders challenged could also be a statistic to report in the future. At the moment not all companies report on national security orders e.g. Twitter continues to challenge the choice of reporting in bands and does not report on national security orders. Some companies e.g. Cheezburger publish canaries to indicate not having received a request rather than reporting in one of the bands. Table 6 provides examples from Google and Verizon’s reports on the data they can be compelled to disclose under the different orders.

Structure 1	Semiannual report that aggregates the number of orders, directives and NSLs into separate categories: <ul style="list-style-type: none"> • Number of NSLs in bands of 1000 starting with 0-999 • Number of customer selectors targeted, reported in bands of 1000 • Number of orders or directives in bands of 1000 • Number of customer selectors under orders, in bands of 1000 • Number of orders for non contents reported in bands of 1000 • Number of customer selectors targeted under orders for non contents under this Act, reported in bands of 1000
Structure 2	Semiannual report that aggregates the number of orders, directives and NSLs into separate categories: <ul style="list-style-type: none"> • Number of NSLs in bands of 500 starting with 0-499 • Number of customer selectors targeted, reported in bands of 500 • Number of orders or directives in bands of 500 • Number of customer selectors under orders, in bands of 500 • Number of orders for non contents reported in bands of 500 • Number of customer selectors targeted under orders for non contents under this Act, reported in bands of 500
Structure 3	Semiannual report that aggregates the number of orders, directives and NSLs into separate categories: <ul style="list-style-type: none"> • Total number of all national security processes received, including NSLs, and orders and directives under this Act, reported in bands of 250 starting with 0-249 • Total Number of customer selectors targeted under all national security processes, reported in bands of 250
Structure 4	Annual report that aggregates the number of orders, directives and NSLs into separate categories: <ul style="list-style-type: none"> • Total number of all national security processes received, including NSLs, and orders and directives under this Act, reported in bands of 100 starting with 0-99 • Total Number of customer selectors targeted under all national security processes, reported in bands of 100

Table 5. Limitations on FISA orders and NSL Reporting in the USA Freedom Act

	NSL	FISA
Google	What does an NSL compel Google to disclose? Under the Electronic Communications Privacy Act (ECPA) 18 U.S.C. section 2709, the FBI can seek “the name, address, length of service, and local and long distance toll billing records” of a subscriber to a wire or electronic communications service. The FBI can’t use NSLs to obtain anything else from Google, such as Gmail content, search queries, YouTube videos or user IP addresses.	Under the Foreign Intelligence Surveillance Act (FISA), the government may apply for court orders from the FISA Court to, among other actions, require U.S. companies to hand over users’ personal information and the content of their communications.
Verizon	The FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. The FBI cannot obtain other information from Verizon, such as content or location information, through an NSL. Verizon does not release any other information in response to an NSL, such as content or location information.	A FISA order for content could compel Verizon to intercept voice communications or provide the government with stored content. What is a FISA order for non-content? A FISA order for non-content is an order that compels Verizon to produce call detail records or similar “transactional” information about communications carried on Verizon’s networks, but does not require Verizon to produce any content.

Table 6. Descriptions of data that can be disclosed under national security requests, taken from Google’s Transparency Report.

Reporting on Offenses Associated with Law Enforcement Requests:

Reporting on the offenses associated with types of orders can also help enhance the transparency of the reports while also allowing for an evaluation of law enforcement practices. For the wiretap orders, it would be similar to the categories of crime listed within the wiretap report. The Wiretap Report provides the type of crime associated with a particular order but the transparency reports are largely deficient in this regard. Tumblr’s report (Tumblr, 2015) provides some transparency in the form of publishing the categories of requests where it did not inform users of the requests (2015). It breaks these down into categories such as suicide, privacy, harassment etc. Once more and more companies start reporting, it would be easier to determine what type of offenses law enforcement is targeting and to check the effectiveness against other statistics publicly available such as those on the arrests made for drugs in a year. Complete reporting on the number of arrests or incriminating evidence obtained using the data made available by companies would have to be initiated by the government in order to be able to evaluate the effectiveness of the law enforcement practices.

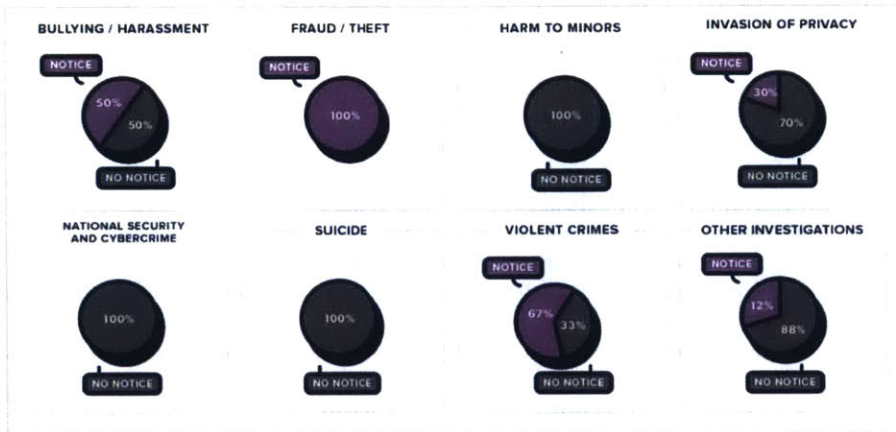


Figure 6. Screenshot from Tumblr's Transparency Report (2015)

Reporting on Internal Processes for Handling Requests

Qualitative reporting on process handling for different requests is another feature that must be present in the overall transparency effort by companies in order to be able to understand the level of scrutiny that a company exerts in processing requests. This may also help a company review its internal practices and develop better methods across different offices and cover any loopholes that may exist in the system. Google's transparency webpage features a video clip (Google, 2014) that takes the user through the entire process that Google uses from when it receives the request to when and how it discloses data.

Transparency Report Model

Companies must begin to become more and more specific regarding the requests they make. Given the prevailing best standard for each type of information, Table 7 provides a list of components to be included in a transparency report.

Category	Reporting
For Search Warrants, Subpoenas, Court Orders e.g. 18 USC 2703(d)	Qualitative: <ul style="list-style-type: none"> • Definition of each process. • Type of data disclosed under each process. Quantitative (report separately for each type of process): <ul style="list-style-type: none"> • Number of orders • Number of people specified in the orders • Number/Percentage of orders complied with • Number of people impacted as a result of compliance • Numbers on reasons for noncompliance: request was too broad, no data was found etc. • Numbers or percentages of the types of data disclosed (e.g. content vs. non-content) • Numbers/Percentages of requests pertaining to certain categories of Offenses • Number of requests from each U.S. state • For subpoenas: number of civil v. criminal subpoenas

Wiretap Orders, Pen Registers/ Trap & Trace Orders	<p>Qualitative:</p> <ul style="list-style-type: none"> ● Definition of each process. ● Type of data disclosed under each process. ● Legal requirement to <p>Quantitative (report separately for each type of process):</p> <ul style="list-style-type: none"> ● Number of orders ● Number of people specified in the orders ● Number/Percentage of orders complied with ● Number of people impacted as a result of compliance ● Numbers on reasons for noncompliance: request was too broad, no data was found etc. ● Numbers or percentages of the types of data disclosed (e.g. content vs. non-content) ● Numbers/Percentages of requests pertaining to certain categories of Offenses ● Average number of days of tapping for each order and/or report number of orders for the following categories: <15 days, 15-30 days, 30-60 days, >60 days ● Number of state v. federal requests ● Number of requests from each US state
Law Enforcement Agency Requests	<p>One of the following:</p> <p><i>Per Order Reporting:</i> Name of the agency making the request</p> <p><i>Aggregate Reporting:</i> Numbers of requests made by different agencies</p>
Emergency Disclosures	<p>Number of requests</p> <p>Number/percentage of compliance</p> <p>Crime/cause leading to emergency</p> <p>Numbers on the type of data revealed</p> <p>Requesting Agency* (if without a nondisclosure order)</p>
NSLs	<p>Qualitative: Report on the type of information provided in response to NSLs</p> <p>Quantitative: Report in bands, using one of the options from the USA Freedom Act:</p> <ul style="list-style-type: none"> ● Number of requests ● Number of accounts affected <p>Content v Non Content (%)</p>
FISA Orders	<p>Qualitative: Report on the type of information provided in response to NSLs</p> <p>Quantitative: Report in bands, using one of the options from the USA Freedom Act:</p> <ul style="list-style-type: none"> ● Number of requests ● Number of accounts affected <p>6-month delay in reporting to comply with the legal requirement.</p> <p>Content v Non Content (%)</p>
Supplementary Statistics	<p>For previous years, the numbers or ranges (if NSLs or FISA orders) of orders with expired non-disclosure orders. Report for each year separately.</p>
International Requests	<p>For each country, report on the following:</p> <p>Number of requests</p> <p>Number of people/accounts specified</p> <p>Number of requests where some data was produced</p> <p>Number of people impacted</p> <p>Number or percentage of content vs. non-content</p> <p>Agency making the request</p>

Table 7

Conclusion

The varying granularities, standards and formats in transparency reports make it difficult to aggregate data and provide an overall account for industry wide surveillance. Varying granularity in data also makes it difficult to tell stories about data and to compare the performance of different companies on their handling of user requests. One form of analysis that can be done is observing trends in each company over time and this is only possible for a limited set of companies that have been publishing data for more than a year. Several statistics if provided by all companies, can improve the overall utility of the reports as tools for public policy and advocacy. The model transparency report presented in this chapter provides a standard that companies need to strive towards. The next chapter in this thesis looks at the various factors that influence companies when publishing transparency reports and identifies the tools that can be used by stakeholders to push companies into becoming more transparent.

Chapter IV

Improving Transparency Reports

But when governments or corporations abuse their power, the commons can act as a counterweight and support network through which citizens can carve out the necessary spaces to speak and organize, and thus defend their rights and interests.

- Rebecca MacKinnon

“As long as this data can only be seen on a piecemeal, company-by-company basis it's impossible to gauge the larger picture” (Peterson, 2014). The previous chapter highlighted a number of problems emerging from the lack of standardization of reports across the industry. The absence of a governance framework makes it difficult to force companies into adopting a particular standard of reporting. Bruce Schneier regards these reports as primarily PR motivated to “reassure us that only a small percentage of user data is being sent to the government” (2015). But can these reports actually become more useful? This chapter identifies the factors that push companies into publishing and improving transparency reports. Moreover, it evaluates several tools and processes that stakeholders can use to assess transparency reporting practices and impose pressure on to companies in order to promote more granular and standardized reporting across the industry. The digital commons is the virtual equivalent of Tocqueville's civil society (MacKinnon, 2012) and therefore, there are ways in which the civil society can come together to protect its rights and in this case develop techniques to hold companies accountable.

Transparency reporting has resulted in fostering a healthy competition among companies and is increasingly being looked at as a performance metric. The very act of publishing a transparency report leads to companies evaluating themselves and recognizing the internal processes that endanger the privacy of their users. Some companies began to improve the way they dealt with government requests and some produced customized tools to handle them (Budish, 2014a). For example, one company used to keep track of government requests for user data in an e-mail in box in one country and used different methods in other countries with little coordination between offices (Budish, 2014b). Creating a transparency report required them to change the

manner in which they dealt with requests and added consistency to the way they responded to requests from all over the globe (Budish, 2014b). Similar changes may have occurred for other companies and transformed their internal processes and perhaps, even in depth discussions on the status quo.

Reports can help companies exert more scrutiny on the data requests they respond to, as it would affect their compliance rate that they publish in the report. This may also lead to the development of better internal accountability processes. It has also been observed that company employees feel excited about such reports as it's a positive contribution their company makes for the society and investors are also increasingly becoming interested in transparency reports (Budish, 2014a). Publishing numbers that would be visible to a variety of stakeholders should convince companies to become more responsible in their behavior as the slightest mishap could result in criticism from all sides, damaging the reputation of the company.

Publishing reports also helps companies gain approval from civil rights and advocacy groups such as the EFF and thereby, boost the image of the company in the eyes of the civil society and the public at large. While publishing transparency reports can have a favorable or adverse affect on the company, the reports have the ability to push companies into acting more responsibly and resisting government pressure to a higher degree. Before the Snowden leaks, most companies were unwilling to share data on the government requests that they received and the sheer number of companies reporting since 2013 lends credence to the favorability of transparency reporting in the eyes of the companies. In 2009 when Yahoo objected to a FOIA request asking for it to release information for compensation it received for surveillance it stated that disclosure of the information could be used to 'shame' Yahoo! and other companies and would "shock" their customers, leading to impairment of its reputation for protection of user privacy and security, which is a competitive disadvantage for technology companies"(Gershberg, 2009).

Reports also attract attention from users and assists in building user trust in the platform and its services. "Transparent business practices engender consumer trust and, by acting transparently, companies can distance themselves from the government and its actions" (Samway, 2014). Transparency reports have sparked conversations online on Twitter and Facebook. Companies do try to keep some track of the effect the report is having on the user base. Tumblr posts its report on its blog and keeps track of

the reblogs and questions that it is asked online regarding the reports (Kazemi, 2014). Credo Mobile emails its transparency report to a mailing list of over 3 Million people (Bond, 2014) in order to promote readership. Typically the media catches the report and creates stories about the data. This helps to improve the readability and reachability of the reports but also has the potential to distort the true nature of the report readers would interpret the numbers through the lens of an intermediary. Tumblr's report aims to target users directly and so the report features easy to understand graphs accompanied with text and annotations describing what the data means. Many of the companies already publishing reports are equipped with resources that allow them to heavily invest in advertising their report online, in stark contrast to the AO that only uploads the reports to the website and depends on the media to carry it across to appropriate channels.

There is a great deal of competition amongst companies in finding ways to become more transparent. This is an important factor that will continue to ensure that transparency reports evolve over time and that there is "a race to the top rather than a race to the bottom" according to Cynthia Wong¹⁶. After Apple published its report in 2015, Nate Cardozo, staff attorney at EFF commented on how reports were becoming an industry standard: "if you want to be taken seriously as a tech company that respects its users, you need a transparency report" (Cardozo, 2015). Company representatives believe that publishing reports "doesn't even feel like an option any more - it's the norm" (Freedom Online Coalition, 2015).

As the reports become the bare minimum standard in the industry, some companies are trying harder to do more by publically fighting the government to legally allow more transparency. The race to the top and the need to rebuild user trust after the Snowden leaks has also resulted in companies pushing the government into allowing them to become more transparent. Twitter spoke out against the limitations imposed on it from disclosing the number of NSLs and FISA orders that it received even if the numbers were zero (Lee, 2014). Twitter is currently challenging the U.S. government on First Amendment grounds for restricting it from disclosing the exact number of requests under these legal frameworks rather than reporting in ranges. This is particularly important because it is challenging the limitation to reports in bands under the USA Freedom Act. If Twitter is successful, numbers of orders will be a lot more

¹⁶ In a discussion with Cynthia Wong dated 25th March 2016

illustrative of the actual scale of requests than they are at the moment. Since the allowance of reporting in bands, many companies have begun reporting on national security orders and if the limitation is removed, companies would be able to publish in numbers.

There have been other instances of companies rallying together to impose greater pressure against the government to allow for greater transparency. This points towards a great deal of room for collaboration apart from the healthy competition that transparency reports cultivate. “While respondents view doing privacy “well” as a strategic advantage in the marketplace, they are also cognizant that a peer’s mistake risks tarnishing the entire sector or worse by drawing regulatory or public attention” (Bamberger & Mulligan, 2015). Therefore, there is an incentive to work together and protect the entire industry. For example, Google, Microsoft, Yahoo and Facebook sued the U.S. government to loosen the restrictions imposed on them against publishing detailed transparency reports (Kopstein, 2013) and managed to get the support of a number of companies and civil advocacy groups. It was partly the efforts of the companies that resulted in the USA Freedom Act allowing more opportunities for companies to become transparent regarding the national security orders that they receive.

The current “market” for transparency reports seems to have reached a critical mass¹⁷ of companies. Companies that want to begin publishing transparency reports do not need to start from scratch and can rely on the existing pool of reports and resources available. Companies can choose to adopt a format or standard found in many of the reports available in the market and customize it according to the “look and feel” of their own company without the assistance of a large legal team. The best practice would be to find the format providing the most specificity that is relevant to the type of requests that the company faces. Companies can also contact the EFF or the ACLU for assistance in the process without exhausting their resources. Credo Mobile, for instance, took help from the EFF at zero cost when it decided to publish its transparency report (Bond, 2014). Some companies that already publish reports may also be willing to help newcomers in the transparency-reporting sphere (Budish, 2014).

The Transparency Reporting Toolkit by OTI and the Harvard Berkman Center helps companies create transparency reports and is primarily targeted towards

companies that have yet to publish reports. The recently published memo by the team identifies the current best practices for transparency reporting across the industry. The team has also been presenting a 'template' for transparency reporting at different conferences and workshops to help more companies ease into the process of reporting. The template is still in its draft stage and is being piloted before it is made publicly available (Budish, 2016). The resources "will be shared publicly to foster standardization in reporting and provide companies new to reporting with an easy-to-use set of tools essential to crafting" (Woolery et al., 2016). In my conversation with Ryan Budish, who is leading the effort from the Berkman Center's side, the toolkit is primarily aimed at companies who are yet to publish reports and he feels that big companies that already publish reports are less likely to be flexible in changing the format of their reports. However, more generally their goal is to get companies into changing their transparency reports so that they become more effective and have clearer definitions. The toolkit should also help companies that err on the side of caution though limited transparency to become more comfortable in reporting at a more granular level. The team has been receiving positive feedback from companies that they have interviewed while preparing the toolkit but they have yet to hear from a company that promises to adopt their model for reporting requests. The memo and template were a product of two years of effort and since the framework has been established, scaling up in the future to include newer reports would not be as resource intensive for the group (Budish, 2016). The group however, has not planned future steps as yet and still has to decide the frequency with which it will be publishing newer reports over the next few years. The effort is likely to have a strong impact on transparency reporting as it drives down costs for companies who seek to publish reports and the best practices identified can become a reputable standard to strive towards or act as a "stamp of approval" for a company's reporting practices.

Inculcating greater competition within the market for transparency reporting can be essential in driving companies towards better reporting. With increased transparency, there is a need to develop metrics that allow users, investors and civil liberties groups to be able to compare company performance over time and against one another. EFF's "Who Has Your Back?" Report and Ranking Digital Rights Corporate Accountability Index rank companies on a number of components in their transparency reports and policies. These reports act as tools for stakeholders to measure company

performance and incentive companies into doing more. Both efforts have been praised by almost all of the experts that I had discussions with and they regard these as steps in the right direction on the road towards greater transparency.

The Electronic Frontier Foundation's (EFF) "Who Has Your Back?" Report was first published in 2012 with the aim of examining whether companies stand on the side of users when government attempts to get access to their data and to allows users to make informed decisions about the companies they trust. The Report evaluates companies on five criteria (Electronic Frontier Foundation, 2015): industry accepted best practices, telling users about government data requests, publically disclosing the company's data retention policies, disclosing the number of times governments seek the removal of user content or accounts and the company's compliance rate, and pro-user public policies (e.g. opposing backdoors). It uses a star-point system to rate each company and complements the rating with a qualitative description that justifies the given score. The most recent report scores 23 companies with 9 of them receiving 5 stars. Over the years EFF has been raising the bar on performance so that companies continue to strive and improve.

These scorecards are useful in many ways but also impose costs on EFF. I contacted EFF to inquire about the costs associated with the report. The EFF regards the process as resource intensive as the team not only scours the publicly available information made available by the company but also contacts the companies to ask for more information regarding certain practices¹⁸. When asked about the scalability of the process in light of an increase in transparency reporting, EFF commented on the usefulness of transparency reports in providing them with information but the process still remains resource intensive. The future of the report seems to be uncertain in terms of whether EFF would want to increase the number of companies it reviews. However, a sample of companies and an improvement in transparency performance can perhaps, have a ripple effect on other companies in the industry and in gradually setting industrial norms and practices.

¹⁸ In conversation with Rebecca Jeschke, Media Relations Director and Digital Rights Analyst at EFF.












	Follows industry-accepted best practices	Tells users about government data demands	Discloses policies on data retention	Discloses government content removal requests	Pro-user public policy: opposes backdoors
	★	★	★	★	★
	★	★	★	★	★
	★	★	★	★	★
	★	★	★	N/A	★
	★	★	★	N/A	★
	★	★	★	★	★
	★	★	★	★	★
	★	★	★	★	★
	★	★	★	★	★
	★	★	★	★	★
	★	★	★	★	★

Figure 1. A Snapshot from EFF's "Who Has Your Back?" Report (2015)¹⁹

Ranking Digital Rights²⁰ (RDR) is an international team of researchers dedicated to building a process to assess, rank and compare the world's most powerful ICT companies on privacy and freedom of expression. RDR issued its first Corporate Accountability Index in 2015 with the aim of evaluating 16 of the world's most powerful ICT companies on their public commitments and policies affecting users' freedom of expression and privacy" (Ranking Digital Rights, 2015). Rebecca MacKinnon, who's at the forefront the initiative, describes the purpose behind the Index to provide advocates with clear information on company practices and how they can improve on their protections with freedom of expression and privacy. This would allow advocates to approach companies on clearly defined ideas on how to improve their policies. In addition, the scores would spark competition among companies into doing more to reach the top of the scorecard. In addition, companies can initiate dialogue with RDR on

¹⁹ This only lists a few of the companies from the report.

²⁰ Ranking Digital Rights is a project led by Rebecca MacKinnon under New America Foundation's Open Technology Institute.

how to improve in the rankings and what more needs to be done at their end (MacKinnon & McGlinchey)

The Index ranks companies on three categories: commitment, freedom of expression and privacy. The indicators are built on the UN Business and Human Rights Framework and the GNI Principles. The rankings rate the companies on a percentage scale based on a number of questions related to each of these categories and provide users and civil society with a list of criteria to look for in companies. Even if the report itself does not cover the broad range of companies that exist in the ICT industry, it provides an array of questions that may be regarded as metrics to measure performance of companies over time and across the industry. The aggregated points for each category can then be used to compare different companies. The “privacy” category looks at companies’ transparency reporting practices and identifies their weaknesses. The statistical data are supplemented with qualitative information on these practices. For example, the Index found Google’s transparency report to be lacking because it does not include requests made via subpoenas from civil court cases involving private parties (Ranking Digital Rights, 2015).

Another interesting feature of the Ranking is that it looks at how the company is structured to provide oversight for companies’ practices affecting freedom of expression and privacy. The “commitment” category in the rankings evaluates companies based on internal governance and management oversight, implementation of mechanisms to protect freedom of expression and privacy (e.g. employee training), multi-stakeholder engagement, commitment towards human rights impact assessment, and the provision of remediation mechanisms. A screenshot from the Ranking shows the total scores for Internet companies (Figure 2).

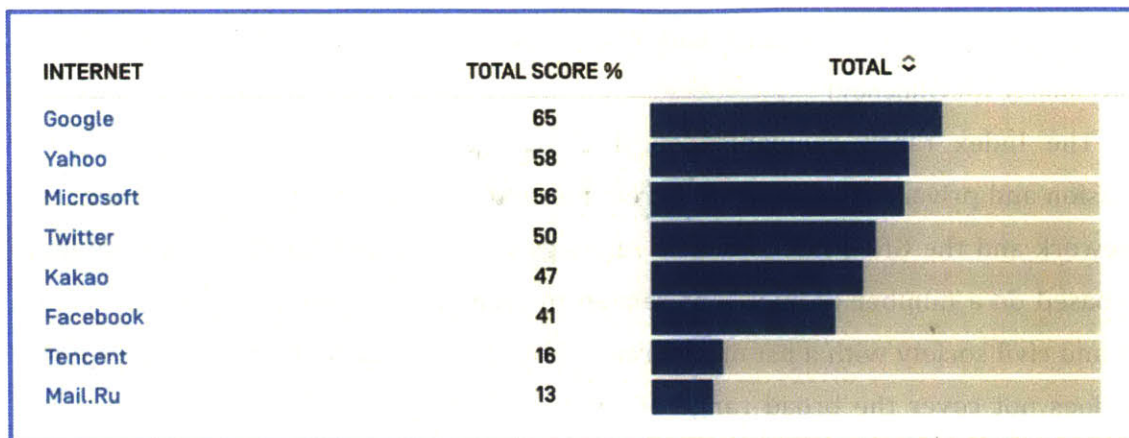


Figure 2. A snapshot of the total score chart for Internet companies in the Ranking Digital Rights Corporate Accountability Index.

A detailed set of questions in the ranking are dedicated to a company's transparency on the requests it receives from the government. The questions cover basic features of transparency reports but can become more detailed with subsequent iterations of the index. The current list of questions is as follows:

- The company breaks out the number of requests it receives by country.
- The company lists the number of accounts affected.
- The company lists the number of pieces of content or URLs affected.
- The company lists the types of subject matter associated with the requests it receives.
- The company identifies the specific legal authority making the requests.
- The company lists the number of requests it complied with.
- The company either publishes the original requests or provides copies to a third-party archive such as Chilling Effects or a similar organization.
- The company reports this data at least once a year.
- The data reported by the company can be exported as a structured data file.

The performance of the reviewed companies under this set of questions is given in Figure 3.

Overall Company Performance

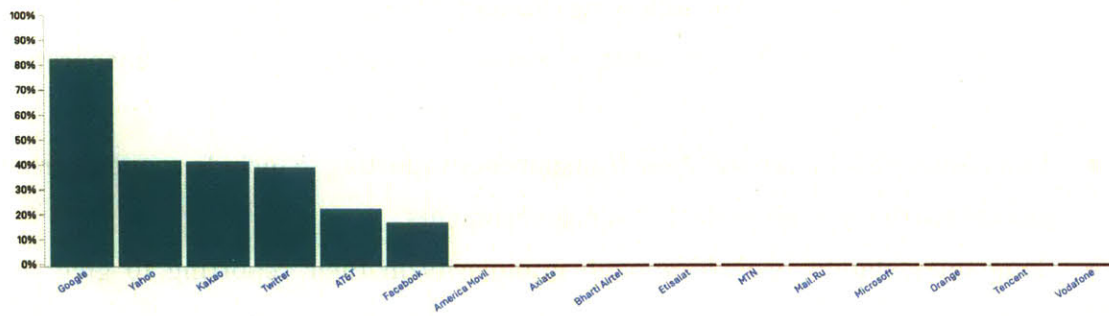


Figure 3. Performance on an RDR question on transparency reporting

All companies do not seem to be performing well in RDR’s book and the percentages show a wide room for improvement. According to MacKinnon, “The highest grade was a D, and that was Google...there’s a lot of room for improvement, all around.” (MacKinnon & Magistad, 2016). RDR conducts greater scrutiny and a higher standard to reach due to the specificity of the questions and the wide scoring range. A comparison of the common set of companies evaluated under both rankings sheds light on the difference and how companies performing well in EFF’s book do not necessarily do well in RDR’s and vice versa (TABLE 1).

Company	“Who Has Your Back?” (2015)	Ranking Digital Rights (2015)
Google	3 stars	65%
Twitter	4 stars	50%
Microsoft	3 stars	56%
Facebook	4 stars	41%
Yahoo	5 stars	58%
AT&T	1 star	50%

Table 1.

A white paper supplemented the RDR report and provides a list of findings and recommendations for transparency reporting. The report points out that there is no

transparency on private requests for user data. The recommendations for transparency on requests for user data were the following (Kumar, 2016).

- Companies should specify what services or platforms their transparency reporting covers.
- Companies should expand their transparency reporting to include requests from private parties as well as those from governments.
- Companies should provide enough granularity in their reporting to give the public a clear picture of the scope and implications of company actions

The creation of the Index is a resource intensive process and therefore, only a sample of companies was surveyed. The estimated cost of RDR for the 2015 Report and data collection efforts was \$300,000 and the budget for 2016 has been estimated to be anywhere between \$400,000 to \$500,000 to evaluate 100 companies (MacKinnon, 2014c). Currently, the pool of companies evaluated does not provide an accurate picture of transparency reporting across the industry and therefore, there is a need to scale up.

EFF's Report inspired Ranking Digital Rights and several other reports. EFF has partnered with local organizations in Latin America, to launch similar reports adapted for local needs and realities (Rodriguez, 2015). In Peru, the "Who Defends Your Data?" Report is a joint initiative by EFF and a local digital rights organization. The report evaluates the privacy practices of digital communication companies that are commonly used by Peruvians. The scoring mechanism involved giving stars to the companies on the basis of their privacy policy and whether it was easy to understand and provided the necessary information, requirement of a judicial warrant by a judge before handing over communications data, promising to inform customers of government requests at the earliest time permitted by law, publishing transparency reports (including information on what type of request, the government agency making the request and the reasons provided), and evidence of commitment to privacy and challenging government legislation permitting mass surveillance (Rodriguez, 2015). The "Who Defends Your Data?" Report in Mexico (Garcia & Rodriguez, 2015) has a similar set of evaluation criteria in addition to rewarding a company's public stance in opposition to mass surveillance. Screenshots from results of the two reports can be found in **Appendix B**.

EFF's methodology also inspired an information policy group in Canada to carry out an evaluation of ISPs operating in Canada on their transparency (Clement & Obar,

2014). The authors comment on having directly modeled their report on EFF's Report but supplementing the criteria with Canadian specific controversies surrounding privacy and civil liberties. The report uses a similar star table and evaluates companies on a number of criteria related to their transparency reporting and disclosure.

Impact of Rankings and Scorecards

Assessing the impact of the reports on company behavior is important and requires a bit of deliberation. In addition to the ripple effect that the scoring and rankings have in launching similar initiatives, there are several ways in which these mechanisms have a broader impact on society and the debate surrounding privacy and transparency. These efforts provide a way for civil society to hold companies and the government accountable in addition to incentivizing positive competition between companies on their privacy and freedom of speech policies and safeguards. The indicators or metrics in the rankings provide relative comparisons between companies and allow civil society to observe changes in company performance over time. Such efforts "counter state influence over the ICT sector precisely so that the Internet can remain a neutral forum for deliberation and debate" (Maréchal, 2015).

Parallels have been drawn between ranking mechanisms in this space with traditional human rights issues such as those of labor and gender equality. Issuing rankings or scorecards is seen as a common activity amongst traditional frameworks and initiatives but the fact that foundations such as MacArthur, Ford, and Open Society support such ranking initiatives is indicative of them having confidence in the rankings being effective to some degree, in changing the behaviors of those being ranked (Maréchal, 2015).

Rebecca MacKinnon has observed that companies in the post Snowden era, are realizing the importance of privacy and security as a selling point and beneficial for profitability, "when you see Tim Cook from Apple standing up to the NSA, he's doing the right thing. But it also happens to be really good for his business" (MacKinnon & McGlinchey, 2016). Sarah Labowitz claims that many investors are becoming increasingly interested in how companies perform on social indicators such as privacy (2016). In addition, she feels that companies, especially big companies do respond to such rankings and they can be internally motivating factors for companies to improve or maintain certain policies. The key question that Labowitz feels is important to ask is

how one measures performance and discerns meaningful differences in companies? These reports provide some ways of drawing comparisons between companies and become tools that civil society and users could use to hold companies accountable and drive demand for certain policies and features that might be present in some companies but not in others. At the core of an ICT company is user trust. As Michael A. Samway, founder of Yahoo's Business and Human Rights program terms it: "These brands are as strong or weak as their practices and their reputations: trust is what makes the wheels go round...these companies know competitors are a click away" (Samway, 2014b). Jeremy Malcolm, senior analyst at EFF described the positive response of companies to their report:

"They [companies] are very competitive at trying to increase their star ranking. Often, we'll give them the opportunity to fix the problems that we found in advance so they don't complain at us afterwards. Many of them do that. So in the lead up and even in the few weeks prior to the release of who has your back, they will improve in terms of service and improve their compliance in certain ways. And even following the release of the report, sometimes that will send them into a complete panic because of the press and they will suddenly comply." (2015)

The practices identified in early reports have become industry standards and EFF is proud to have played its role in pushing companies into the right direction in incorporating the changes that it recommended (Electronic Frontier Foundation, 2015). Change can also be observed over time by looking at the change in ratings since the first report was published. The chart in Figure 4 shows the changes in the stars allotted to a sample of the companies covered by all four reports.

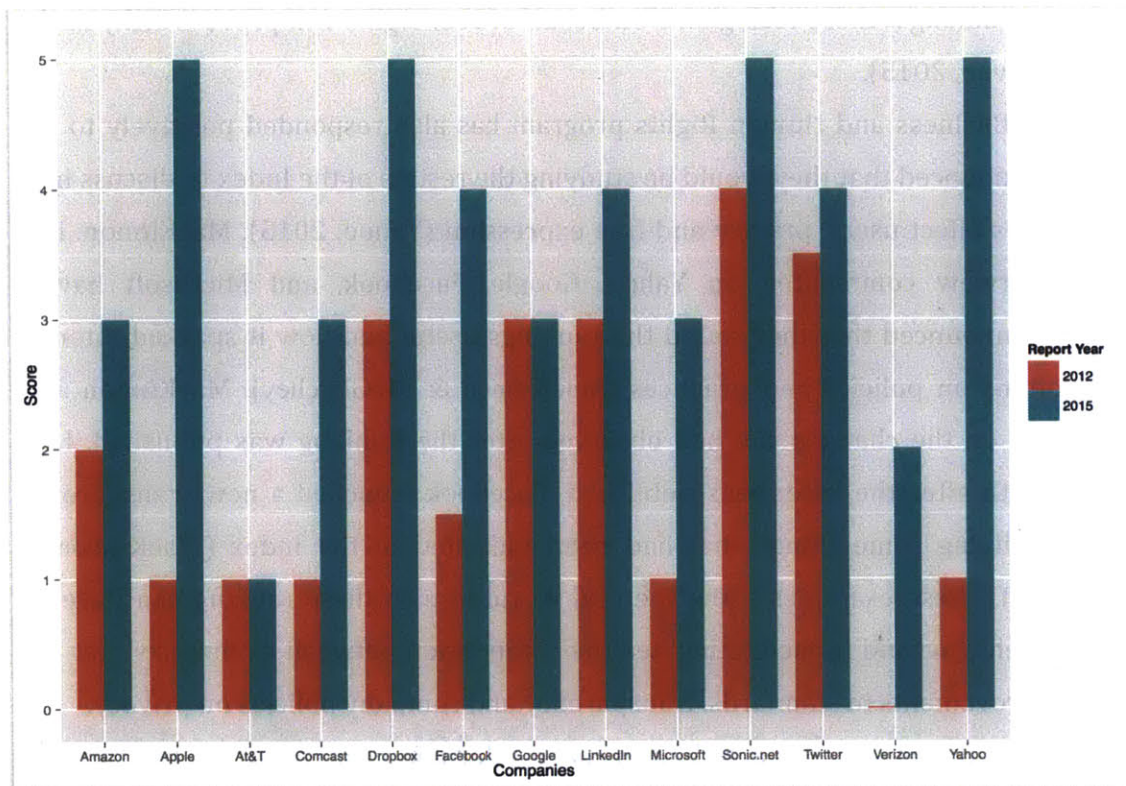


Figure 4

Most companies have performed better on the scorecard since 2012. While it is difficult to attribute the report as the cause, companies have been positively responding to such scorecards and they do affect company policies and practices internally. The Report may also serve to create competition amongst companies and help in creating a standard for reporting that is on par with other companies. At the bare minimum, the rankings help highlight poor performers and encourage them to improve before the next iteration of the ranking, while rewarding better performers with positive media attention (Maréchal, 2015). In addition, with a more aware consumer base, companies would be able to compete with one another on better policies for transparency and privacy. Having a more informed user base enjoying better privacy and freedom of expression will allow more effective advocacy needed for legal reform (Maréchal, 2015).

David Sullivan, an independent consultant for Global Policy, Corporate Responsibility, and Human Rights, believes that the RDR Corporate Accountability Index does provide room for cautious optimism as competition and collaboration may be simultaneously possible when respecting rights (Sullivan, 2015). While some companies have a strong dislike for rankings on human rights and non-financial issues but sparking

competition amongst these tech giants on behalf of user rights will prove worthy in the future (Sullivan, 2015).

The Yahoo Business and Human Rights program has also responded positively to the RDR and announced that they would be studying the results of the Index to discuss how their policies affect users' privacy and free expression (Yahoo, 2015). MacKinnon, in a recent interview commented on Yahoo, Google, Facebook, and Microsoft having publically announced that they found the rankings useful and how it sparked internal conversations on policies and practices (MacKinnon & McGlinchey). MacKinnon also commented on the changes she had observed after the Ranking was published. Less than a month after the index was published, Facebook launched a new transparency report, clarifying some things that had been indicated in the Index (MacKinnon & McGlinchey). These examples show the real world impact these ranking can have on company behavior and in facilitating healthy competition between companies that can lead to improvements in standards, transparency and company policies on privacy.

The rankings and scorecards also make information more accessible to users who might not be willing to spend the time and effort comparing different policies and reports by multiple companies. Corporate disclosure notices and user agreements are written for tech lawyers and regulators (MacKinnon, cited in Thielman, 2015) and therefore, there is a need for there to be an easier way for consumers to be able to make informed choices.

EFF's scorecard and the Digital Rights Ranking were widely publicized in a variety of online news websites and blogs with often alarming and eye-catching headlines such as: "When it comes to privacy, Apple's 'got your back' says EFF" (Evans, 2015) "Tech Firms Trust Our Government Even Less Than You Do" (Pegoraro, 2015), "Tech Titans Score Abysmally On Data-Privacy Rights" (Hackett, 2015), among numerous other headlines. Such articles facilitate discussions on social networking platforms such as Facebook and Twitter and help users get more out of the transparency reports that companies publish.

Above all, the reports provide stakeholders with the tools to assess company performance on different metrics, leading to directed efforts towards companies to improve their performance. Recently, Access Now has launched a campaign directed at 10 companies evaluated under RDR offering them specific recommendations on how to improve their policies and practices (Iancu, 2016).

In conclusion, the process of scoring and ranking companies drives competition and provide a way to hold companies accountable for their policies. These initiatives are constrained by resources and might not be scalable enough to cover the scope of the entire global ICT industry. However, sampling companies and encouraging them to do more should generate ripples within the industry as stakeholders begin to demand the same level of effort as the companies receiving higher scores.

Complementary Tools for Transparency Reports

Transparency reports have given rise to a complementary set of tools that facilitate analysis of transparency reports and are aimed at a variety of stakeholders. This section introduces these tools and reviews their relevance and effectiveness in the transparency and accountability ecosystem.

Silk's Transparency Reports Database

Silk's Transparency Reports Database²¹, contains transparency reports from all major service providers and normalized into a resource that can be used to investigate government requests for data. The toolkit provides users with the ability to generate a number of different visualizations that allow comparisons between countries and companies with regards to government requests for data and company compliance. Civil society, academics, researchers and others can use the tool to generate visualizations of analyses of different metrics without spending a lot of time in gathering and aggregating the data. Data on Silk is kept in the form of data cards that allow users to view the data at a company and country level. The database does not seem to have been updated in the last two years and only contains data cards for 19 companies. The number of companies publishing transparency requests are over 40 now and the database must be updated to be able to reflect the current status quo.

Access Now's Transparency Reporting Index

Access Now's Transparency Reporting Index²² features a record of all transparency reports published by leading Internet and telecommunication companies. The index

²¹ The database is available at the following URL: <https://transparency-reports.silk.co/> last visited 3 April 2016.

²² Available at the following URL: <https://www.accessnow.org/transparency-reporting-index/> Last Visited: 25 April 2016

provides a long, downloadable, table of company names, location of their HQs, type (Internet/Telco), date of first release of transparency report, the frequency of the report and a URL to the report. It provides an easy way of checking which companies have been publishing reports and when to expect the next report from the company. Peter Wright of Access Now shares how the Index has been able to map the trend of transparency reports from the time when they were only a few to now becoming a norm and has served to promote transparency reporting (Wright, 2015). In contrast to the indexes that rank and score companies, this Index is more of a minimum threshold that companies meet simply by publishing a report.

Canarywatch

Many companies use canaries to indicate they have not received certain types of requests from the government and removal of the canary indicates having received such a request. The efficacy of the canary depends on whether people are observing the canary over time. With the increasing number of companies publishing canaries, it becomes difficult to keep track of all canaries and this is where *Canarywatch*²³ becomes a useful tool. A joint project by a number of organizations²⁴, it lists and tracks changes in canaries over time and allows submissions for canaries not listed on the website. As of 21st March 2016, there are 61 canaries being tracked on the website. Canarywatch is another tool in the activist's toolbox that can give a glimpse into the hold the government has on the ICT industry. Changes in canaries can be easily detected and taken up by media, civil society organizations and others to start a conversation.

Saliency, Legitimacy and Impact

Each of these tools and assessment techniques can be viewed and compared using a framework that looks at their saliency, legitimacy, potential impact and the resource requirement. The matrix in Table 2 evaluates each of these through the lens of academics and civil rights/advocacy groups. The Transparency Reporting Toolkit ranks high in saliency due to the elaborate survey that has been conducted of current

²³ <https://canarywatch.org/> Last Accessed March 21st 2016

²⁴ Canarywatch is a coalition of organizations that include the EFF, the Berkman Center for Internet and Society, NYU's Technology Law and Policy Clinic, Freedom of the Press Foundation and the Calyx Institute.

practices in transparency reporting and the findings can be used by civil society to encourage companies to perform better. It also ranks high in legitimacy due to the transparency of the process through the detailed memos and the impeccable reputations of the OTI and the Harvard Berkman Center in this sphere. The impact at the moment is unknown since companies have not responded to whether they will be restructuring their reports as a result. But since the toolkit and the expected template are aimed at making reporting easy, we can expect many companies to adopt their model. If this were to happen, the industry wide impact would be high and a common standard could begin to take shape using the Toolkit's template.

EFF's "Who Has Your Back?" Report ranks high in salience as it evaluates the companies on a number of criteria that advocates and other stakeholders consider relevant and it allows a means for benchmarking company performance on a number of indicators while reducing the cost for individual organizations or experts to carry out the task on their own. EFF's longstanding reputation of advocating for online civil liberties makes the ranking legitimate in addition to the transparency of the process used to score and justify the scoring scheme. Since the number of companies EFF evaluates is low and they have commented on resource constraints, the scalability of the report is low and it might not have a high enough impact that could lead to standardization across the industry. However, it may lead the evaluated companies into doing more and this may or may not have an affect on other companies if they feel that they do not need to in the absence of a score for their own company.

Ranking Digital Rights Index also ranks high in salience and legitimacy. The team behind RDR is a mix of well-known experts in the area and the ranking process and methodology are all very transparent. In addition, the use of multi-stakeholder input when framing the methodology adds legitimacy to the Index. According to Jillian York (EFF), RDR is particularly impressive. She felt that companies performing poorly in the ratings were no surprise and that she has faith in the methodology (York, 2016). Given RDR manages to review a 100 companies as intended in its next iteration, it might have a high impact on company behavior and transparency reporting practices. The resource cost identified is moderate to high and in relative comparison to other tools. RDR has also been receiving feedback from stakeholders particularly at RightsCon²⁵ and this is

²⁵ Rights Con is an annual conference sponsored by Access Now and brings together a large number of experts, company representatives and civil rights groups.

important, as the feedback will loop into the next iteration of the Index and rank even higher in legitimacy.

Silk’s Transparency Reports Database hasn’t been updated in two years and lacks salience as a result even though the legitimacy of the effort is high given the fact that the previously collected data is accurate and that the algorithms in place function well in helping users generate stories. The potential impact is low considering since analysts haven’t used it in a while. Canarywatch is salient since companies continue to use canaries and the platform can help stakeholders keep an eye out for killed canaries. The Transparency Reporting Index is also salient but to a lesser degree since it hasn’t been updated since the end of February to reflect new reports e.g. Uber’s report. If Uber did not feel the need to report to this Index, it might not be well known in the transparency sphere, or at least to companies. Access Now, the organization behind the Index is well reputed and sponsors conferences such as RightsCon. The impact at the moment seems to be low if companies do not consider adding their entry to the list as a top priority. Had Uber’s report been included in the first week of it being published, there might have been a higher degree of optimism.

Tool	Salience	Legitimacy	Potential Impact on Transparency Reporting	Resource Requirement
Transparency Reporting Toolkit	High	High	Mod-High	Moderate
“Who Has Your Back?” Report	High	High	Moderate	High
Ranking Digital Rights Index	High	High	Mod-High	Mod-High
Silk Transparency Reports Database	Low	High	Low	Low
Canarywatch	High	High	Low	Low
Transparency Reporting Index (AccessNow)	Mod	High	Low	Low

Table 2. Saliency, Legitimacy and Impact Framework

The Need For an Aggregation Tool

While stakeholders try to push companies in the direction of better transparency reporting practices there is the need to be able to aggregate data easily in order to have a central repository of all the statistics for industry wide surveillance. Ideally, we would want to see an online toolkit that allows companies to provide numbers for the various processes and for those numbers to be available publicly for interpretation and analysis. Ryan Budish felt that the challenge would be in motivating companies into donating their data to a repository and this would be particularly hard when companies already have set norms for publishing their reports (2016). A project already underway in relation to the Toolkit under OTI operates on a similar principle but allows companies to create their own transparency report on the platform and then generates a repository of standardized statistics. This would primarily target companies that do not produce transparency reports and would like to use a standardized template to get started but it would be difficult to get other companies on board. ACLU, California is also rumored to have a project in place for transparency reporting involving companies reporting each request to the organization but no details have been made publicly available.

Conclusion

The surveillance landscape is very broad and requires a number of tools to build a layer of accountability and transparency in the absence of governance. There is no one tool that can solve the problem of more transparency. This chapter examined the “accountability tools” that can assist civil liberties groups, academics, investors and users help compare the privacy and transparency policies of companies. By inculcating competition in the industry through rankings and scorecards and making it easier to evaluate company practices, stakeholders can rally for better transparency reporting practices. This chapter dealt entirely with the policies that companies make publicly available and there is no way of verifying whether the internal policies of companies match with the statements they make publicly in their reports. The next chapter looks at the platforms that attempt to reduce the governance gap by providing a window into the internal practices of companies.

Chapter V

Global Network Initiative

The GNI's key challenge is this: Given that there is basically no country on earth where the government is not pressuring companies to do things that arguably infringe on citizens' rights, how do companies take practical steps to protect their consumers' and users' rights to free expression and privacy?

- Rebecca MacKinnon

The previous chapter examined the use of tools that can be used to improve transparency reporting in the absence of a governance framework in the industry that can mandate companies to report in a standardized manner. The key limitation of the tools discussed so far is that they only penetrate company policies at the surface level through the information that the latter makes publicly available. As a result, there is no transparency with regards to whether the company handles requests with the policies it publicly claims to uphold. This chapter presents a case study of the Global Network Initiative, a multi-stakeholder platform that seeks to provide a degree of accountability and transparency around the internal policies of companies. However, the internal assessment process of the GNI for assessing companies contains several flaws, which makes it difficult to provide the desired transparency.

While contextualizing GNI's presence in the industry, it is pertinent to start with a brief discussion on multi-stakeholder initiatives. A 'multi-stakeholder initiative' is often used to describe:

"voluntary initiatives where two or more stakeholders cooperate to address some area of sustainability, corporate social responsibility (CSR), the environment and/or human rights. Such stakeholders include some combination of companies, industry associations, non-governmental organizations (NGOs), trade unions, government agencies, investors, academics and international organizations" (Baumann-Pauly et al., 2016).

Multi stakeholder initiatives (MSIs) are born in governance gaps, usually in the aftermath of a "crisis affecting a particular industry" (Baumann-Pauly et al., 2016). In the case of the GNI, a series of multi-stakeholder discussion began in 2006 when U.S.

companies began to receive attention from the government and public with regards to their negative impact on human rights abroad (Laidlaw, 2015). Two particular incidents, which may be seen as catalysts, were: i) Yahoo handing over information on a Chinese journalist to Chinese authorities leading to his arrest and imprisonment and ii) Google launching a censored version of its search engine in China (Laidlaw, 2015). In response to these circumstances, and “largely forced by congressional threat of legislation in 2006” (MacKinnon, 2012), an unlikely group of civil activists, academics, investors and competing companies (Google, Microsoft and Yahoo!) began to take form.

GNI was officially launched in 2008 after about two years of deliberations among the various stakeholders. Joining the GNI became representative of a commitment to internationally recognized laws and standards when dealing with government requests for user data and protecting and respecting the privacy rights of their users (MacKinnon, 2012). One of the goals of the GNI is to allow companies to convince various stakeholders that they can be trusted to not abuse and violate the public interest (MacKinnon, 2012). The companies were facing pressures from different governments and a broad spectrum of laws and so the GNI allowed them to collaborate to push back against them. Their reputations were at stake and this resulted in breeding a collaborative spirit amongst the otherwise fiercely competitive companies. As Colin Maclay puts it, the move was not based on pure altruism but to fix a serious business problem (2010).

The multi-year discussions resulted in a core framework for GNI that was grounded in three documents: the Principles, the Implementation Guidelines and the Governance, Accountability and Learning Framework (Globalnetworkinitiative.org, 2012a). The Principles are based on internationally recognized laws and standards for human rights, including Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (“ICCPR”) and the International Covenant on Economic, Social and Cultural Rights (“ICESCR”)(Globalnetworkinitiative.org, 2012b). The Principles have been divided into the following: freedom of expression, privacy, responsible company decision-making, multi-stakeholder collaboration and governance, accountability and transparency. These helped create the Implementation Guidelines to provide the ICT industry and stakeholders with direction and guidance on how to protect and advance human rights globally (Globalnetworkinitiative.org, 2012c). Last, the Accountability, Policy, and

Learning Framework provides details on the assessment processes that will be used to hold companies accountable (Globalnetworkinitiative.org, 2015).

Edward Snowden’s disclosures resulted in legitimizing the position of GNI, as a framework to fill the governance void for human rights in ICT companies but also pointed towards the weaknesses in the voluntary system of assessments (Laidlaw, 2015). Some of the major companies identified by the disclosures were part of the GNI and it was embarrassing to note that the assessment procedures in place were not able to capture the relationship the companies had with the government. EFF, a founder of the GNI soon departed from the organization in response. The GNI blamed the legal limitations imposed by the government that prevented companies from disclosing the nature of their relationships with the government. The current GNI member base consists of a small set of companies and a number of civil society organizations, academics and investors (Figure 1).



Figure 1. Chart based on membership information of the GNI (Global Network Initiative, 2016)

GNI recently welcomed seven global telecom companies as observers: Millicom, Nokia, Orange, Telefónica, Telenor Group, TeliaSonera, and Vodafone Group. This

development is particularly important as a group of stakeholders that had been largely missing from the GNI member pool will now be actively participating. The observer-ship period culminates in a full-member position at the end of a year.

GNI places a huge emphasis on shared learning through interactions between members and non-members and allowing participants to bring up issues. This allows civil society, academics, investors and companies to raise issues that concern them. GNI also conducts learning forums through annual multi-stakeholder interaction with the Telecommunications Industry Dialogue. Another important interaction that GNI engages in is with the Freedom Online Coalition, an international multi-stakeholder group that brings together a number of different stakeholders including representatives from governments. In its Annual Report for 2014, GNI mentions securing commitments from 24 governments on surveillance transparency as a result of its interaction with the FOC (Global Network Initiative, 2015).

The true power of the GNI lies in the relationships it has created amongst its participants and the potential for the platform to be used to engage with the government. The group provides representation of various stakeholders and has used its strength to take part in policy debates that affect the ICT industry and human rights issues. In a 2012 report entitled “Opening the Lines: A call for transparency from Governments and Telecommunications companies” (Tuppen, 2013). GNI recommends ISPs and governments be transparent about applicable laws and operating licenses, government requests for user content and metadata, government requests for filtering and, government requests for text messages sent via the ISP’s network without attribution. Google’s Transparency Report is said to have been born out of its commitments as a GNI member (MacKinnon, 2012).

Overview of the GNI Assessment Process

The efficacy of voluntary regulation through an MSI depends on the verification of compliance with the standards the company has agreed to adhere to. One of the key contributions of GNI to transparency is that its member companies agree to be audited by independent assessors. This is the only window into the internal human rights practices in an ICT company

According to MacKinnon, GNI’s accountability framework was modeled after existing MSIs such as the Fair Labor Association (FLA) (MacKinnon, 2012). FLA is

comprised of a group of companies, NGOs, and university purchasers of branded apparel and footwear that got together with the aim of working with companies to improve working conditions in garment factories and ensuring violations were reported (MacKinnon, 2012). Other examples include MSIs born out of the extractives sector. The key participants in the initial discussions brought experience from participating in MSIs in these sectors (Samway, 2016). While these models were looked at in order to decide what the GNI should pursue, the assessment process for GNI faced a novel set of challenges.

At the heart of GNI is an assessment framework that was particularly different than those of its predecessor MSIs. This was in part due to the “novelty, complexity, and global scale of the ICT industry” (Samway, 2016). The initial stage of the assessment framework involves self-reporting by the company after one year of membership. This is followed by an independent assessment of each company member every two years by a board-approved independent assessor. The report goes through multiple stages. The first stage involved redacting commercially sensitive information from the report before sharing it with the Executive Director of the GNI and then a more redacted version with the rest of the GNI board, which then votes on the company’s compliance with the standard (Baumann-Pauly et al., 2016). GNI completed its assessments for its three founding companies, Google, Yahoo! and Microsoft in 2013. However, the published report on the assessments (Global Network Initiative, 2014) only contains aggregated information with very little details on the individual performance of each company.

The assessment process also adopts a case study methodology that looks at how companies respond to certain types of requests. The total number of cases that were addressed across all 59 companies and 29 of them pertained to requests for user data.

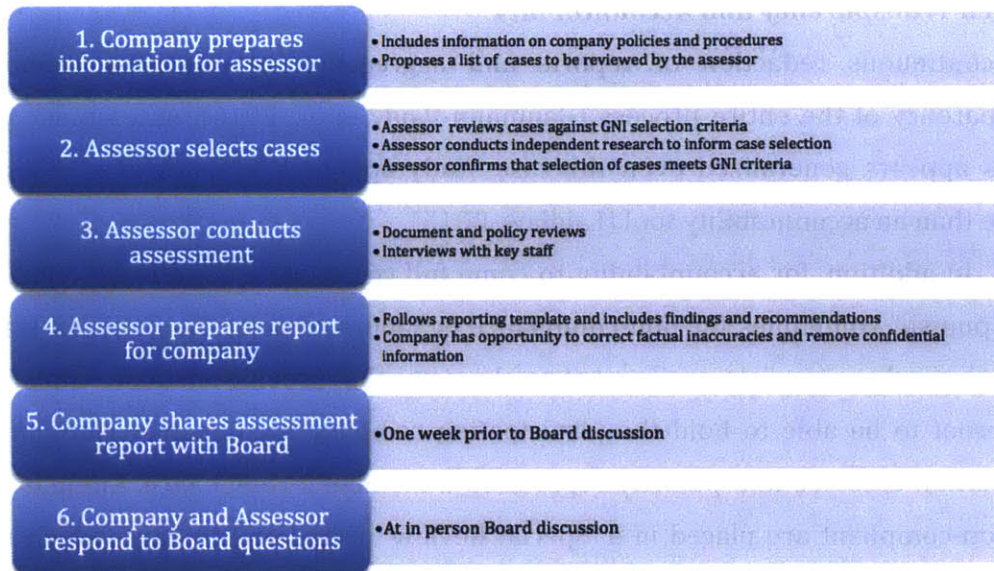


Figure 2. Steps of the GNI Assessment Process (Source: GNI 2014 Assessment Report)

The process culminates with a vote from the GNI Board on the compliance status of the company and a report to the public. Required contents of the different reports are given in the chart below (Table 1):

Independent Reporting to the GNI	Assessor Reporting to the GNI	GNI Reporting to the Public	Company Reporting to the Public
Summarizes the assessment, the relevant facts, corrective action plans (if any), and recommendations for improvement.	Qualitative evaluation of strengths, weaknesses, and opportunities for improvement in the processes the company has put in place to implement the Principles and a summary of conclusions for the GNI.	<p>A summary of the progress made by GNI and member companies.</p> <p>Collective lessons learned regarding the Principles and Implementation Guidelines, including examples of the types of requests received.</p> <p>Information required to improve the understanding of threats to freedom of expression and privacy across different sectors, geographies, legal systems, and cultural traditions.</p> <p>For each participating company undergoing an assessment that year, the GNI Board's compliant or noncompliant decision</p>	Using a format of their own choosing, each participating company will within six months of the end of an assessment communicate to the public about the outcome of their assessment.

Table 1.²⁶

²⁶ Table created using information available on the GNI website for the Framework (Globalnetworkinitiative.org, 2015)

Limited Transparency and Accountability

The continuous redaction of reports and aggregation of outcomes reduces the transparency of the entire process (Baumann-Pauly et al., 2016). Assessment in most places appears generalized even the case study approach is more of a reassurance device than an accountability tool (Laidlaw, 2015).

In addition, for accountability to come full circle, there need to be mechanisms that “punish” companies for non-compliance or failure to meet the required standard. This required appropriate assessment mechanisms that provide adequate transparency and proof to be able to hold the participating company accountable. The Fair Labor Association assesses and publicly reports on a member’s compliance. Companies that are non-compliant are placed in a ‘Special Review’ period of 120 days, which may be followed by a termination from the MSI if the FLA board votes to do so²⁷. The period may also be extended for as long as it is needed for the company to address the problem that has been identified. GNI’s assessment process in comparison appears to be rudimentary as indicated by the report on the assessment and seems to be focusing more on the “process of assessment than the companies being assessed”(Baumann-Pauly et al., 2016). GNI seems to be lacking with regards to a sanctioning mechanism such as the one developed by FLA. In the initial days of the GNI, civil society and investors were particularly concerned that there should be real consequences for non-compliant companies over time. (Samway, 2016) Currently, companies can be placed on special review for an appointed period of time, which can be extended depending on how long it will take the company to remedy the situation. But perhaps, criticism by internal and external stakeholders may be enough to trigger remediation steps as it appears, GNI seems to be more like a platform where others can point fingers at a company for not doing enough.

The case study approach that GNI uses, draws instances from the pool of thousands of requests received by the company and the assessor cannot know the full scope of the requests and whether the company responded in the same manner for all requests of the same type. Companies can choose to disclose whatever they are comfortable with and cite a number of reasons if they are not able to do so. Some cases that may make the company look bad or if a company feels particularly concerned about

²⁷ FLA, ‘Charter Document’ (as amended 12 February 2014), www.fairlabor.org/sites/default/files/a_charter_2-12-14.pdf. cited in Baumann-Pauly, 2016.

others finding out, will never make it to the assessment pipeline and the auditor would remain in the dark.

Legal obstacles add another layer of secrecy around the requests received by companies and unless the government allows greater transparency, no audits will be able to penetrate a company's human rights impact to its entirety. Non-disclosure orders can continue to prevent companies from providing the assessor with more information.

Conflict of Interest and the Potential for Biases in the Assessment Process

The potential for biases to seep in throughout the assessment process also inhibits accountability. One of the stakeholders I met with regarding the GNI, felt that there is bias due to funding sources, which can weaken the credibility of the assessment process and the GNI as a whole. Conflicts of interest exist in the assessment process at two points in the chain. First, the tech companies being reviewed pay the accredited organizations assessing the company and the report is usually filtered before it makes its way to the GNI. While this process is usually done to remove sensitive information from the report, it could also lead to other changes, which would go unnoticed by the board members that review the watered down version of the evaluation. The GNI does attempt to exercise caution in ensuring that the assessor is independent and lays out a number of criteria in its Independence and Competency Criteria (Global Network Initiative, n.d.) for accredited assessors. The document covers a number of factors that may lead to conflicts of interest for the assessor e.g. relationship with a GNI employee or board member, investments in the company being assessed etc. So the problem truly arises at the point when the company decides to remove what it feels should not be seen by the GNI Board and this may lead to reduced transparency.

Second, representatives of civil society organizations present on the GNI Board regularly receive grants from the GNI companies. Center of Democracy and Technology (CDT) is a regular recipient of grants from Facebook, Google, Yahoo!, LinkedIn and Microsoft²⁸ since 2009²⁹. Similarly, another organization on the Board, "Index on Censorship" is sponsored by Google and Vodafone, a new entrant to GNI list of companies. GNI does take particular caution in ensuring that none of the independent

²⁸ Analysis of the CDT Funding Charts between 2009-2013 reveal contributions from all of these companies (cdt.org, n.d.)

²⁹ LinkedIn began funding CDT in 2010.

assessors carrying out internal assessments have conflicts of interest, it does not allude to any biases that may be present within the GNI Board, which eventually votes on the status of compliance.

While this is in no way meant to criticize the organizations or individuals participating in the assessment process or to imply that these companies are not neutral, assessments must be truly independent in order for them to be credible and this involves removing any potential biases that might seep into the process.

Sarah Labowitz feels GNI's independent assessment process is flawed and assessments should be conducted by an internal GNI assessment team (2016). But GNI is restricted by the pool of resources it has. Currently, GNI has a budget of approximately \$733,295 for running the organization that is supported by the annual membership fees that companies pay (Baumann-Pauly et al., 2016). An internal assessment team would be very costly but companies that pay for independent assessments could instead contribute to the GNI resources assessments. However, during the initial days of GNI, companies could not agree on allowing GNI to audit them.

Time Lags

The GNI assessment process is supposed to be conducted every two years, which is a long time in the context of an industry that is developing at a fast rate with frequent interactions with law enforcement and an evolving and reactionary regulatory landscape. For instance, when the first independent assessment report came out in the beginning of 2014, companies could not say anything about their NSLs but soon after they were allowed to report in bands. The public would then have to wait for two years before behavior related to the NSLs could be unearthed. Frequent assessments could have allowed more insight into the behavior that companies were not allowed to talk about previously.

Report Visibility

Another challenge that MSIs face is in communicating assessment results to the non-member stakeholders at large: the public, investors, consumers among others and many MSIs have had difficulty in transforming the information into indicators that may be easily understood and allow comparisons of member companies (Baumann-Pauly et al., 2016). EFF's "Who Has Your Back?" Report and Ranking Digital Rights' Corporate

Accountability Index make company evaluations easy to understand. Rebecca MacKinnon, is also one of the founders of the GNI and recognizes the difference Ranking Digital Rights makes in providing a comparison between companies and its edge over the GNI: ““It’s [GNI’s assessment] a pass-fail, so that’s one reason why I wanted to do the ranking,” “It’s more than a pass-fail. It’s a real grade” (MacKinnon & Magistad, 2016). By scoring and ranking companies on their performance, the reports are easily understood by a wide variety of stakeholders and are consumed quickly by online media and forums. The GNI at the moment is particularly lacking in the way it presents its results to the public and this reflects a problem within the process.

Absence of Key Stakeholders

GNI cannot be seen as representative of the entire ICT industry given the small number of member companies and the absence of key organizations from the platform. The addition of telecom industries has filled much of the void that had long existed in GNI but there is still no representation of a US telecom company in the GNI. Twitter continues to be absent from the GNI but continues to show its commitment to protecting privacy and freedom of speech by challenging the government and becoming more and more transparent through the evolution of its transparency report. Without being able to rope in major companies of the industry, GNI’s role and influence in a greater transparency reform is highly unlikely.

EFF left GNI in 2013 soon after the Snowden disclosures and cited the breakdown in the confidence it had in the GNI due to the limitations imposed on transparency by the government on companies from disclosing information about their practices (Electronic Frontier Foundation, 2013). Jillian York, who co-authored the letter of resignation to the GNI feels that to this day, GNI has made very little progress and a completely different and independent approach to company assessments needs to be considered³⁰.

Amnesty International, a well known human rights advocacy group also decided not to join GNI as it did not place enough confidence in GNI due to a number of issues remaining unresolved over the two years of deliberation (Johnson, 2008). NYU Stern’s Business and Human Rights Center recently departed from the GNI. Sarah Labowitz and Michael Posner who represented the Center at GNI felt that several gaps in the structure

³⁰ In my discussion with Jillian York dated 28th March 2016

should have been changed before allowing telecom companies into the initiative (Posner & Labowitz, 2016).

Hardware manufacturers like Cisco have not joined the group despite pressure from civil society and the government and attributed their refusal to fundamental differences in their business models compared to other participants and their internal and external commitments to human rights (Samway, 2016). While Cisco is not a member company, it has publicly commented on its support for the GNI principles and the work that it does.

Due to the departure or absence of key stakeholders, GNI is not truly representative of the ICT industry. Therefore, any efforts fostering standardization that do take place will not be able to influence the entire industry. “The GNI needs to bring on board more companies, earlier stage companies and more companies from outside the U.S.” (Samway, 2016)

Lack of Resources

GNI’s ability to influence company and government decisions on free expression and privacy depends on it building and sustaining the human, capital and organizational resources to staff and finance its core functions (Samway, 2016). Currently, GNI has three staff positions and is primarily funded by the annual membership dues. This limits the impact it can have as a platform for engagement and in hiring a pool of top talent in the area.

Recommendations

The GNI in its current state cannot provide ideal accountability and transparency due to its assessment framework. Many of the respondents to questions on GNI were critical of the process and the future of the GNI. But for now, GNI is the only platform within the ecosystem that has the capability of peering into a company’s internal practices for ensuring respect for privacy and freedom of expression. Under the status quo, GNI cannot provide reliable assessments. However, it can be useful in standardizing a certain set of practices and definitions across the small pool of companies that it has as members. The companies and stakeholders already a part of GNI can adopt standards that can trickle down to other non-member companies in the industry. This would mimic the “best in class” approaches found in industrial settings (Baumann-Pauly et al.

2015). An epitome of this phenomena is Google's Transparency Report of 2010 followed by a number of reports that kept on raising the bar for reporting standards in the industry (Baumann-Pauly et al., 2015). In addition to competition another pushing factor would be the civil society and other stakeholders as they impose pressure on companies to adopt the same standard.

Baumann-Pauly et al., argue "if a critical mass of players in one industry defines and adopts rules, they can jointly create a new level playing field." (2015) This brings us to the question of what the critical mass for the ICT industry looks like. The researchers argue that GNI meets the criteria of having a critical mass as defined by the "collective leadership potential to re-define the rules of the game" (Baumann-Pauly et al. 2015). Market leaders, therefore, have the capability of transforming the landscape.

I strongly believe that GNI has not acquired a critical mass due to the absence of major companies belonging to different categories within the industry. Hardware manufacturers, surveillance technology manufacturers, major US telecom companies among other groups, are missing from the dialogue. Different types of companies have their own norms in terms of their relationships with the government. In addition, underlying business practices and infrastructure may change the nature of the relationship. Once the critical mass of companies is acquired, any standards that are adopted are no longer voluntary but become the de-facto binding on the companies (Baumann-Pauly et al. 2015). The authors recognize the need to have telecom companies and hardware companies on board in order to broaden its impact.

In order for GNI to have a more significant impact in the ICT industry in terms of setting standards and norms for transparency reporting and practices, a number of actions may need to be taken:

1. Standardizing internal processes and definitions for receiving and dealing with government requests. Requests should be stored in a standard manner across all companies using the most specific title for each type of request. Similarly, categories could be created for non-US companies with common terminology across all companies so that they may be able to report finer details for non-US requests.
2. Requiring each company to report transparency statistics in the most granular manner - as defined by the maximum standard for reporting allowed by law. Since the reports are public, GNI would not require extra resources to check for

compliance. OTI and Berkman Center's Transparency Reporting Toolkit can provide details on the best standard available for each category.

3. An independent system of assessments that is not tainted by possible biases stemming from conflicts of interest. Labowitz recommends an internal GNI assessment team. However, most companies in the initial stages of GNI were uncomfortable with the idea of assessments being conducted by GNI. We do need to realize that the process is not very transparent. Need to rethink of a solution that would allow more insight and transparency into a company's internal processes without threatening their trade secrets.
4. Imposing pressure on the government to allow greater transparency and to publish its own transparency reports.

Freedom Online Coalition

Some attention also needs to be devoted to another MSI that exist in the industry, the Freedom Online Coalition (FOC). The FOC is a partnership of 29 governments that engage with the private sector and civil society to advance and support Internet freedom. FOC's Working Group on Privacy and Transparency Online (WG3) is of particular relevance to this thesis as it concentrates on the relationship between governments and ICT companies on respecting human rights online, especially freedom of expression and privacy (Freedom Online Coalition, 2014). WG3 is comprised of experts from ICT companies, governments, civil society and academia from around the world. In November 2015, the group published a report that "examined the role of transparency as a tool for government and corporate accountability, and as a fundamental part of empowering individuals to fully exercise their rights online, including freedom of opinion and expression" (Freedom Online Coalition, 2015). The group aims to: i) define a multi-stakeholder definition of transparency that covers corporate and government transparency, ii) Analyze emerging issues, and iii) develop models for more robust government transparency reporting.

Unlike the GNI, the FOC working group does not have an internal assessment process but rather engages the different stakeholders to obtain their inputs on the issues that they face on different fronts. For example, the group has been able to uncover a number of constraints and incentives that companies face when publishing

reports. In addition, it is able to get the opinion of different governments on transparency reporting.

The working group primarily seems to be in an advisory capacity and stakeholders can learn from the reports and voluntarily adopt some of the standards that the report identifies, however no commitment can be binding. Nevertheless, it provides a platform for companies and stakeholders to come together and devise a format for transparency reporting that may be acceptable to most parties.

Conclusion

The GNI and the FOC WG3 are incapable of setting common standards throughout the industry but are valuable in their efforts to understand the pressures that companies face internally. However, both companies lack the critical mass of companies that may be necessary to sway the entire industry into reporting in a standardized manner. In addition, while GNI aims to provide some transparency and accountability concerning internal processes of companies when facing requests, it is at the moment incapable of providing sufficient transparency that may allow stakeholders to place trust in companies and the requests that they may receive from governments.

Chapter VI

Reducing Limitations on Transparency Reporting

“The public should not have to rely on the disclosure of classified orders, such as the Snowden leak, for important information regarding invasions of their privacy by government surveillance.”
(Correia, 2014)

Most of this thesis thus far, has focused on corporate transparency reports, which operate within legal constraints framed by the government and only provide a partial picture of the surveillance landscape. Without knowing the full extent of the different programs, a democratic society is limited in its ability to make informed choices and decisions. (Losey, 2015) In this context, it is impossible to discuss greater transparency of surveillance mechanisms without addressing the need for government to allow greater corporate transparency and to publish its own reports on its requests for user data. While companies have taken strides in improving the transparency of the requests they receive, the government has fallen short even though it has an important role to play. This chapter describes the need for transparency reports to be published by the government, evaluates the existing mechanisms the government has in place for transparency reporting, and identifies efforts by stakeholders demanding greater transparency from the government.

Corporate transparency reports in their current form, do not provide an overall picture of the surveillance landscape and there have been many calls from across the stakeholder spectrum demanding that the government do more in terms of transparency reporting. The government has a special role to play in generating greater transparency:

Government agencies are positioned to provide information on how different legal justifications are used by different agencies, what type of data is collected, and the extent that data collection takes place by different agencies. Increased government reporting would support accountability on how the interpretation of

specific laws is being used, and on the extent that surveillance changes between reporting periods. (Losey, 2015)

“Greater transparency by governments about requests and requirements being placed on companies that have the potential to affect Internet users’ freedom of expression and privacy is a prerequisite for accountability in public governance of the Internet.” (UNESCO, 2014) Government issued transparency reports can provide industry wide statistics if reported in an aggregate manner or at the granularity of orders issued to each company. In the latter case, a mechanism for two way accountability will be set up as any discrepancies between the numbers reported by the companies or the government would be scrutinized by academics, the public and the civil society.

The Freedom Online Coalition Report shows that company feel that governments are in a better position to provide “a comprehensive picture of requests from all operators” and that they should also provide information on the numbers of orders with gagging orders (Freedom Online Coalition, 2015). Some of the recommendations in the report regarding public disclosure are as follows Freedom Online Coalition, 2015):

- Disclose to the public the legal authorities and processes through which requests to companies are made, and what information can be obtained/ restricted;
- Clarify which government offices/officials have the authority to make requests of companies
- Clarify the permitted uses for information obtained through a request (e.g., disclosing in criminal trials how information was obtained)
- Strengthen qualitative transparency about laws, policies, and processes
- Pursue ways to make this information more accessible. This may involve centralizing reporting on a common website, and contextualizing it for a general audience

The wave of transparency reports has been accompanied by attempts to impose pressure on the government for greater surveillance transparency. Companies have been urging the U.S. government to lift gagging laws that prevent them from disclosing statistics on national security orders that they receive while also demanding the government to become transparent about its practices as well. In the storm following the Snowden disclosures, Google began mounting pressure on the government and was soon joined by Facebook, Microsoft and Twitter (Shih and Rigby, 2013). A number of

companies joined the call for surveillance reform through a coalition called: Reform Government Surveillance³¹. The coalition identified a number of Principles that it felt were necessary and included one on transparency that identified the need for the government to promptly disclose data on number and nature of demands for user information and to allow companies to publish them as well (Reform Government Surveillance, 2013). A letter by the coalition to the senate asked for it to do more in terms of adding transparency and preventing bulk collection of metadata.

Another set of principles, the Necessary and Proportionate Principles were formulated by a group comprising of civil society, privacy and technology experts under the auspices of the UN Human Rights Council. The Principle on transparency require states to publish “aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each.”(Necessary and Proportionate, 2013) In addition, the Principles also emphasize the role of states in steering clear of any interference with service providers “in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.” (Necessary and Proportionate, 2013)

While reporting on government requests for user data, companies do not necessarily face restrictions for warrants, subpoenas and requests under ECPA. The real inhibitors of corporate transparency are restrictions related to FISA orders and NSLs issued by intelligence agencies. From the standpoint of the intelligence agencies, non-disclosures can be justified on the grounds that the target may realize he or she is being surveilled and this may hamper the investigation or targets may deduce the strategy intelligence agencies use and alter their behavior accordingly (Knox, 2016). Similarly, warrant canaries, if tripped can also alert a suspect and lead them to switch services (Knox, 2016). While intelligence agencies, clearly have a justifiable need for non-disclosure orders in many cases, these should be targeted and there must be sufficient transparency for the public to be able to hold agencies accountable for mass surveillance.

³¹ An effort by AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo! RGS: URL: <https://www.reformgovernmentsurveillance.com/>

In January 2014, the Department of Justice (DOJ), allowed two options for reporting FISA orders and NSLs (Table 1). The first option allowed companies to disclose NSLs and FISA orders separately in bands of 1000 and the second option allowed companies to lump both types of processes together and report in bands of 250. These options were then “upgraded” in the USA Freedom Act, allowing four types of reporting structures for companies to choose from.

Option 1	<p>A provider may report aggregate data semi annually in the following separate categories:</p> <ul style="list-style-type: none"> ● Number of NSLs reported in bands of 1000 starting with 0-999 ● Number of customer accounts affected by NSLs, reported in bands of 1000 ● Number of FISA orders for content, reported in bands of 1000 ● Number of customer selectors targeted under FISA content orders, reported in bands of 1000 ● Number of FISA orders for non content, reported in bands of 1000 ● Number of customer selectors targeted under FISA non content orders, reported in bands of 1000 ● Six month delay for FISA reporting ● 2 year delay for “New Capability Order”
Option 2	<ul style="list-style-type: none"> ● Total number of national security processes received including NSLs and FISA orders reported as a single number in the band 0-249 and thereafter in bands of 250 ● Total number of customer selectors under national security processes including NSLs and FISA orders reported as a single number in the band 0-249 and thereafter in bands of 250

Table 1

Twitter, unhappy with the initial settlement only allowing companies to report NSLs and FISA orders in bands, sued the U.S. government on First Amendment grounds in October 2014 continues to stand its ground even after the USA Freedom Act (Lee, 2014). The current version of Twitter’s report does not reveal any statistics on national security requests and continues to challenge the gagging orders in the legal system. Recently as of April 2016, Microsoft has filed a complaint in Seattle’s US district court calling the ECPA unconstitutional in allowing limitless gagging orders³² and violating the First Amendment rights of companies and Fourth Amendment rights of those being “searched”(Microsoft v. Lynch, 2016). In its complaint, Microsoft alleges that in the past 18 months, “federal courts have issued nearly 2,600 secrecy orders silencing Microsoft from speaking about warrants and other legal process seeking Microsoft customers’

³² Some requests are accompanied with gagging orders with no time limit.

data; of those, more than two-thirds contained no fixed end date” (Microsoft v. Lynch, 2016). It appears to be that the authorities have adopted non-disclosures as a default rather than issuing them in special circumstances when there is a legitimate threat in the disclosure of an order. It also points towards the need to reform the laws in cyberspace. Non-disclosures are particularly dangerous for companies that may not have the legal capacity to challenge them. Emerging startup companies particularly in the IoT sector can be exploited by law enforcement and gagged from saying anything concerning the requests that they receive.

Limitless non-disclosure orders continue to hinder transparency efforts as a substantial percentage of the orders that a company receives may be tied with a non-disclosure or “gagging” order. Under such orders, companies may be prevented from even mentioning that they have received such an order or reporting numbers of such orders. In the USA Freedom Act, the government requires non-disclosure orders to be based solely on danger to national security or interference with an investigation and allows companies to challenge nondisclosure orders. However, there is no mention of expiration time of non-disclosure orders in the Act.

Courts also must play a role in ensuring that orders do not remain sealed forever. Brian L. Owsley, a former magistrate judge routinely signed on several sealed orders on the request of the United States Attorney because they involved ongoing criminal investigations. Owsley describes the intuition behind non-disclosure orders is to prevent the suspect in a criminal investigation from being alerted but argues that eventually the orders should have been unsealed (2014). In 2013, Owsley decided to unseal many of the orders that he had signed on over the years and notified the United States Attorney. Owsley however, was stopped by a District Court judge who squashed his orders for disclosure. This points to a need for the courts to become willing to unseal such orders when the need to disclose them subsides. It is difficult for federal prosecutors to reexamine long-concluded cases while they focus on present investigation and prosecution of criminal activities (Owsley, 2014). This points towards the need of decreasing the cost for federal prosecutors if they are to unseal old non-disclosure orders or allow magistrate judges to unseal orders after a specific period of time. Perhaps keeping an electronic record of each order and linking it to a timer that expires after a certain period of time can alert judges without having to go through undisclosed past orders in order to find which ones to disclose. There needs to be a

push from either the courts or the prosecuting officials towards greater transparency and in determining who should bear the burden of unsealing orders. Owsley claims that many judges do not care about the issue of unsealing orders but if they did, magistrate judges and district judges could unseal orders and expose them to the public after a certain period of time. Currently it doesn't seem like there is a "policy window" that might attract the attention of the Congress into enacting legislation related to unsealing nondisclosure orders and the public must exert pressure on to the Government and create that window.

In order challenge these gagging orders, companies must continue to challenge them on First Amendment grounds. Companies have already been challenging the gagging laws on reporting quantitative numbers and although the bands allowed by the USA Freedom Act do help enhance transparency, they are still unable to provide a more accurate picture of the scale of NSLs due to non-disclosure orders that hide many NSLs from the numbers. While these numbers are important to transparency, they are insufficient in providing an idea of what is being demanded from companies using NSLs. (Manes, 2016) First Amendment is particularly relevant because the gagging orders are content based restrictions on freedom of speech and can be likened to classic orders of prior restraint that are forbidden by the First Amendment. (Manes, 2016) Recently, in *Merrill v. Lynch*, the courts successfully overturned a gagging order related to an NSL. This points towards a future where gagging orders are challenged and scrutinized by the judicial system. Companies must continue to challenge gagging orders that appear unreasonable and law enforcement and intelligence agencies must allow gagging orders to expire after a stipulated time. Companies can then publish numbers related to the NSLs as supplementary data for previous years. However, the structures of the bands would make such changes less noticeable and companies must continue to strive for greater allowances on reporting.

The government has on various occasions, emphasized that the class of speakers whom NSL gags suppress is very small. (Wexler, 2014) The USA Freedom Act's provision of allowing companies to challenge non-disclosure orders is likely to shed light on the true nature of the government's claims. Widespread challenges against NSLs are likely to "overwhelm the courts and inhibit the current scale of NSL usage" (Wexler, 2014) in addition to proving the government false.

In addition to allowing companies to become more transparent by reducing the limitations on publishing data pertaining to requests, the government must also produce its own reports. The decentralized structure of surveillance leading to multiple agencies demanding data may result in an abuse of power as agencies continue encroaching on civil liberties. The USA Freedom Act contains reporting requirements for the Director of National Intelligence and the Administrative Office of the US Courts to publicly report on the number of national security orders and estimate of the people affected by them. The Office of the Director for National Intelligence (ODNI) has established 'IC on the Record', a repository for declassified documents, official statements, speeches, and testimonies as part of its transparency efforts (2014). The effort is praiseworthy and has resulted in 5000 documents being disclosed and a number of aims and priorities the office has for greater transparency. The initiative particularly stresses on clear communication to the public and stakeholders via multiple platforms and training programs to integrate better transparency practices into the system. The Office has also begun to publish statistical transparency reports on the numbers of FISA orders and NSLs (Tables 2 and 3). The table listing numbers of FISA orders also provides the estimated number of people affected but does not contain numbers of orders, which may have been denied, or a percentage of approved orders from the total number of orders. Such a statistic would allow the public to know if the orders are being scrutinized.

Legal Authority	Annual Number of Orders	Estimated Number of Targets Affected
FISA Orders based on probable cause (Title I and III of FISA, Sections 703 and 704 of FISA)	1519 orders	1562
Section 702 of FISA	1 order	92707
FISA Pen Register/Trap and Trace (Title IV of FISA)	135 orders	516

Table 2.

Legal Authority	Annual Number of NSLs Issued	Annual Number of Requests for Information
National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709	16,348	33,024

Table 3.

The numbers on NSLs issued and the number of requests for information have been said to vary as the NSLs may be demanded under different authorities for the same person or for multiple facilities (e.g. telephone lines, multiple email accounts etc.) associated with them. IC on the Record has drawn the attention of the Freedom Online Coalition WG3 as an effort towards transparency by the government.

While these numbers provide long awaited transparency, company reporting of such orders needs to be accurate and without bands in order to be able to verify these numbers. In addition, unlike the Wiretap Report, these reports do not provide any information on effectiveness of the surveillance mechanisms. Numbers of arrests and convictions resulting from these orders must also be looked into. The fear of underreporting remains due to decentralization and perhaps, there is a need for a central repository that agencies must submit details of requests to in order for them to be compiled in the annual report.

The USA Freedom Act also introduces requirements for the AO to file an annual report listing the number of orders requested, granted, modified and denied by the courts and to make the report publicly available on a website. The Wiretap Report has been shown to have evidence of underreporting and there is a danger that the same might happen with FISA orders. The discrepancy between the number of wiretap orders in the Wiretap Report and the numbers reported by companies in their transparency reports gives us reason to question the validity of the numbers being reported the courts and prosecutors. Similarly, there is a need to fact-check the number of FISA orders being reported and the limitation of reporting in bands prevents verification of these numbers and points towards the necessity of allowing companies to report in numbers.

Another suggestion that has been made for FISA transparency is to provide the public with the identity of the judge assigned to each case in addition to publishing court opinions on past orders (Correia, 2014). The Wiretap Report does provide names of state and federal judges authorizing the orders and this information could be particularly useful if a method of accountability for unsealing non-disclosure orders is to be initiated.

There are limitations other than national security concerns that prevent the Government from becoming more transparent. One finding is that some governments feel that the process is resource intensive with regards to the time and effort required.

(Freedom Online Coalition, 2015) Co-ordination among agencies issuing FISA orders and NSLs can be costly but a one time investment in a central record keeping system can channel the numbers into a report making body responsible for publishing the report at the end. This will also result in challenges related to privacy and security of the data being shared. The internal methods for tracking and reporting requests must be standardized across all agencies in order to have accurate reporting and to increase accountability.

The Government usually makes decisions on issues that are particularly salient at a certain point in time. One such policy window is emerging in the near future with the expiration of Section 702 of FISA, in 2017. The law is notoriously known for its disparate impact on certain groups, particularly immigrants who may have frequent conversations with individuals living abroad. One suggestion to curtail mass surveillance of certain regions is to provide location statistics pertaining to the orders with reporting delays, if necessary to protect national security interests. Location statistics by the Government would help add a further layer of analysis and accountability of these requests.

Paul Schwartz recommends the creation of an annual “telecommunication surveillance index” instead of publishing different reports (2008). This suggestion ties many of the recommendations made in this chapter into a tool that can provide better oversight. Schwartz provides a number of steps that must be taken in order to be able to publish such a report. The first task involves changing statutes in a manner that the AO of the US Courts collects all the statistics as it does for the Wiretap Report. However, before this suggestion of Schwartz is undertaken, there needs to be an investigation to understand the reason for the large discrepancy between the number of wiretaps reported by the AO and those by companies publishing number of wiretap orders they have received³³. Another step that Schwartz suggests is for the report to cover orders under the SCA as well. In addition, all jurisdictions must be asked to submit a report on wiretap orders even if they have not received any. Chris Soghoian points out that better reporting through such a report card can provide the Congress on information needed to make sound policy in the area (2011).

³³ The numbers of orders for 2014 in the 2014 Wiretap Report and the numbers of wiretaps reported for 2014 by 6 companies are markedly different. This discrepancy was alluded to in earlier chapters to indicate the need for dual accountability.

While the Government has begun to redeem itself to a slight degree with the USA Freedom Act, it still has a lot to do in order to break the legal chains that restrict company reporting and prevent the public from being better informed. In addition, it must keep enhancing the transparency standards of its own reporting mechanisms to allow the opportunity for public debate resulting in feedback loops into policy decisions.

Chapter VII

Recommendations

This chapter serves to summarize all the key takeaways for companies, civil society and the government in order to improve the level of transparency of requests made to ICT companies so that there may be a greater degree of oversight and accountability.

For Companies

- Produce annual or semi-annual reports providing detailed qualitative and quantitative data on the requests received by law enforcement and intelligence agencies with the deepest granularity legally possible.
- Companies with small legal budgets should seek help from EFF and ACLU when publishing reports.
- Companies should use standardized templates such as those provided by the Transparency Reporting Toolkit when beginning to publish reports.
- Support and donate to a central repository for all surveillance requests made to companies from the government.
- Push for greater transparency in the reports using the template provided in this thesis.
- Challenge limitless non-disclosure orders in court on First Amendment grounds.
- Push government into allowing greater transparency on national security orders.
- Assist other companies in producing transparency reports and share ways of dealing with issues and challenges.

For Civil Society, Academia and the Public

- Encourage companies to publish transparency reports on an annual or semi-annual basis

- Encourage companies already publishing reports to report at deeper levels of granularity
- Create a repository for storing data related to surveillance in the industry and encourage companies to donate to the repository
- Evaluate company performance on transparency through evolving rankings and scorecards to facilitate comparisons and encourage competition amongst companies.
- Offer assistance to companies wishing to publish reports by providing legal guidance.
- Conduct workshops and training sessions to assist companies into publishing better reports.
- Encourage the government to become more transparent in its practices and to produce an annual report of the different types of surveillance.

For Government

- Change laws to discourage limitless non-disclosure orders.
- Set up a process to efficiently deal with companies challenging non-disclosure orders and to provide more transparency.
- Create an annual surveillance report providing numbers under different legal statutes and collected by the AO of the US Courts.
- Conduct an assessment to identify the reasons for the large discrepancy between wiretap orders reported by the AO and those by companies and use the information to transform the Wiretap Reporting requirements if needed.
- Require judges to annually submit reports for their jurisdictions even if they do not authorize any wiretaps.

Bibliography

- Access Now., 2016. *Transparency Reporting Index - Access Now*. [online] Available at: <https://www.accessnow.org/transparency-reporting-index/> [Accessed 7 Mar. 2016].
- Apple, 2013. *Report on Government Information Requests*. [online] Available at: <http://www.apple.com/legal/privacy/transparency/requests-20131105-en.pdf> [Accessed 7 Feb. 2016].
- AT&T, 2014. *Transparency Report*. [online] Available at: Verizon, (2014). United States Report. Transparency Report. [online] Available at: <http://www.verizon.com/about/portal/transparency-report/us-report/> [Accessed 8 Apr. 2016]. [Accessed 8 Apr. 2016].
- Balkovich, E. et al., *Understanding the Mobile Ecosystem and Applicable Surveillance Law*, Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR800/RAND_RR800.pdf [Accessed March 8, 2016].
- Bamberger, K.A. and Mulligan, D.K., 2015. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. MIT Press.
- Baumann-Pauly, D., Nolan, J., Van Heerden, A.D. and Samway, M., 2015. Industry-Specific Multi-Stakeholder Initiatives that Govern Corporate Human Rights Standards—Legitimacy Assessments of the Fair Labor Association and the Global Network Initiative.
- Baumann-Pauly, D., Nolan, J., Labowitz, S. and van Herdeen, A. 2016. Defining and implementing human rights standards industry by industry. In: D. Baumann-Pauly and J. Nolan, ed., *Business and Human Rights: From Principles to Practice*, 1st ed. New York: Routledge, pp.107-120.
- Berkman Centre for Internet and Society, 2016. "DON'T PANIC" - Making Progress on the "Going Dark" Debate. [online] Available at: https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [Accessed 6 Apr. 2016].

- Bond, B., 2014a. *Transparency Reporting for Beginners (RightsCon 2014)*. [video] Available at: <https://www.youtube.com/watch?v=QMyaV9yGpco&list=PLprTandRM960PUyig8SUxOViRicZztcFv&index=5> [Accessed 5 Jan. 2016].
- Budish, R., 2014a. *Transparency Reporting for Beginners (RightsCon 2014)*. [video] Available at: <https://www.youtube.com/watch?v=QMyaV9yGpco&list=PLprTandRM960PUyig8SUxOViRicZztcFv&index=5> [Accessed 5 Jan. 2016].
- Budish, R., 2014b. *Transparency Reporting as a tool for Internet Governance (Internet Governance Forum)*. [video] Available at: <https://www.youtube.com/watch?v=Us4BW1Sw4Vo&list=UUk0zf4oI0IsJLh1oWvUQSfQ> [Accessed 5 Jan. 2016].
- Budish, R., 2016. *Discussion on the Transparency Reporting Toolkit*.
- Canarywatch.org., 2016. *Canarywatch*. [online] Available at: <https://canarywatch.org/> [Accessed 23 Mar. 2016].
- Cardozo, N., 2015. | *Electronic Frontier Foundation*. [online] Electronic Frontier Foundation. Available at: <https://www.eff.org/mention/apple-lifts-veil-secrecy-transparency-report> [Accessed 7 Mar. 2016].
- Cdt.org., n.d. *Financials | Center for Democracy & Technology*. [online] Available at: <https://cdt.org/financials/> [Accessed 4 Jan. 2016].
- Clement, A. and Obar, J.A., 2014. Keeping internet users in the know or in the dark: An analysis of the data privacy transparency of Canadian internet service providers. *Available at SSRN 2491847*.
- Congressional Record, 1996. Available at <https://www.congress.gov/congressional-record/1996/2/9/senate-section/article/s1166-2?q=%7B%22search%22%3A%5B%22%5C%22wiretap+report%5C%22%22%5D%7D&resultIndex=1>
- Congressional Record, 1999. Congressional Record Volume 145, Number 145 (Friday, October 22, 1999)][Senate][Pages S13051-S13054] From the Congressional Record Online through the Government Publishing Office <https://www.gpo.gov/fdsys/pkg/CREC-1999-10-22/html/CREC-1999-10-22-pt1-PgS13051-3.htm>

- Congressional Record, 2009. Available at <https://www.congress.gov/crec/2009/10/28/CREC-2009-10-28-pt1-PgH12006.pdf>
- Correia, E.R., 2014. Pulling Back the Veil of Secrecy: Standing to Challenge the Government's Electronic Surveillance Activities. *Temp. Pol. & Civ. Rts. L. Rev.*, 24, p.185.
- CREDO Mobile., 2014. *Transparency - Past Reports: CREDO Mobile*. [online] Available at: <http://www.credomobile.com/transparency-previous-reports> [Accessed 7 Mar. 2016].
- Diffie, W. and Landau, S., 2007. *Privacy on the line: The politics of wiretapping and encryption*. MIT press.
- Dropbox. 2015., *Dropbox - Transparency Report*. [online] Available at: <https://www.dropbox.com/transparency> [Accessed 7 Apr. 2016].
- Electronic Frontier Foundation, 2013. EFF Resigns from Global Network Initiative. *Electronic Frontier Foundation*.
- Electronic Frontier Foundation., 2015. *Who Has Your Back? Government Data Requests 2015*. [online] Available at: <https://www.eff.org/who-has-your-back-government-data-requests-2015> [Accessed 7 Jan. 2016].
- Evans, J., 2015. When it comes to privacy, Apple's 'got your back' says EFF. *ComputerWorld*. [online] Available at: <http://www.computerworld.com/article/2937395/security0/when-it-comes-to-privacy-apple-s-got-your-back-says-eff.html> [Accessed 8 Feb. 2016].
- EPIC, 2014. Title III Wiretap Orders - Stats. *EPIC - Title III Wiretap Orders - Stats*. Available from: https://epic.org/privacy/wiretap/stats/wiretap_stats.html [Accessed January 6, 2016].
- Fakhoury, H., 2012. EFF Tells Supreme Court that No Means No in Wiretap Act. [Blog] *EFF Deeplinks Blog*. Available at: <https://www.eff.org/deeplinks/2012/02/eff-tells-supreme-court-no-means-no-wiretap-act> [Accessed 7 Feb. 2016].
- Fenton, J., 2015. Activists: US overstates encryption threat, under reports wiretap figures. *Aljazeera America*. [online] Available at: <http://america.aljazeera.com/articles/2015/7/17/overstating-encryption-threat-underreporting-wiretap-numbers.html> [Accessed 11 Feb. 2016].

- Freedom Online Coalition., 2015b. Available at: <https://www.freedomonlinecoalition.com/> [Accessed January 12, 2015].
- Freedom Online Coalition, 2015. *Working Group 3 Privacy and Transparency Online*, Available at: <https://www.freedomonlinecoalition.com/wp-content/uploads/2015/10/FOC-WG3-Privacy-and-Transparency-Online-Report-November-2015.pdf>.
- Freedom Online Coalition, 2014. WG 3 – Privacy and Transparency Online. *Freedom Online Coalition*. Available at: <https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-3/> [Accessed Jan 4, 2016].
- Froomkin, A.M., 2000. The Death of Privacy? *Stanford Law Review*, 52(5), p.1461. Available at: <http://www.jstor.org/stable/1229519?origin=crossref>.
- Garcia, L. and Rodriguez, K., 2015. New Report Shows Which Mexican ISPs Stand With Their Users. [Blog] *EFF Deeplinks Blog*. Available at: <https://www.eff.org/deeplinks/2015/06/new-report-shows-which-mexican-isps-stand-their-users> [Accessed 8 Mar. 2016].
- Gershberg, M., 2009. *Freedom of Information Act Request No. 2009USMS13662*. [email].
- Gidari Jr, A., 2006. Companies Caught in the Middle. *USFL Rev.*, 41, p.535. Available at: http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/usflr41§ion=28.
- Gidari, A., 2015. *Wiretap Numbers Don't Add Up*. [online] Just Security. Available at: <https://www.justsecurity.org/24427/wiretap-numbers-add/> [Accessed 7 Mar. 2016].
- Global Network Initiative, 2014. *Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo*. [online] Available at: <http://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf> [Accessed 3 Jan. 2016].
- Global Network Initiative, 2015. *2014 Annual Report*. GNI Annual Reports. [online] Available at: <https://globalnetworkinitiative.org/sites/default/files/2014%20Annual%20Report.pdf> [Accessed 3 Jan. 2016].
- Global Network Initiative, n.d. *Independence and Competency Criteria*. [online] Available at: [http://globalnetworkinitiative.org/sites/default/files/GNI%20Independence%](http://globalnetworkinitiative.org/sites/default/files/GNI%20Independence%20Criteria.pdf)

- 20and%20Competency%20Criteria%20for%20Assessors.pdf [Accessed 4 Jan. 2016].
- Globalnetworkinitiative.org., 2012a. *Global Network Initiative*. [online] Available at: <http://globalnetworkinitiative.org/> [Accessed 3 Jan. 2016].
- Globalnetworkinitiative.org., 2012b. *Principles - Global Network Initiative*. [online] Available at: <http://globalnetworkinitiative.org/principles/index.php> [Accessed 3 Jan. 2016].
- Globalnetworkinitiative.org., 2012c. *Implementation Guidelines | Global Network Initiative*. [online] Available at: <http://globalnetworkinitiative.org/implementationguidelines/index.php> [Accessed 3 Jan. 2016].
- Globalnetworkinitiative.org., 2015. *Accountability, Policy, and Learning Framework | Global Network Initiative*. [online] Available at: <https://globalnetworkinitiative.org/content/accountability-policy-and-learning-framework> [Accessed 3 Jan. 2016].
- Google, 2014. *Way of Warrant*. [video] Available at: <https://www.youtube.com/watch?v=MeKkHxcJfh0> [Accessed 8 Apr. 2016].
- Google, 2015. *United States - Google Transparency Report*. [online] Available at: <https://www.google.com/transparencyreport/userdatarequests/US/> [Accessed 8 May 2016].
- Greenberg, A., 2012. *Here's How Often AT&T, Sprint, And Verizon Each Hand Over Users' Data To The Government*. [online] Forbes.com. Available at: <http://www.forbes.com/sites/andygreenberg/2012/07/09/by-the-numbers-heres-how-often-att-sprint-and-verizon-hand-over-users-data-to-the-government/#5dfea0c11378> [Accessed 7 Mar. 2016].
- Hackett, R., 2015. Tech Titans Score Abysmally On Data-Privacy Rights. *Fortune*. [online] Available at: <http://fortune.com/2015/11/03/google-facebook-privacy/> [Accessed 8 Feb. 2016].
- Iancu, C., 2016. Access Now launches advocacy campaign based on Corporate Accountability Index. [Blog] *Ranking Digital Rights*. Available at: <https://rankingdigitalrights.org/2016/04/14/access-now-launches-advocacy-campaign-based-corporate-accountability-index/> [Accessed 16 Apr. 2016].

- IC ON THE RECORD, 2014. *IC ON THE RECORD*. [online] Available at: <http://www.icontherecord.tumblr.com/> [Accessed 2 Apr. 2016].
- Johnson, B, 2008. Amnesty criticises Global Network Initiative for online freedom of speech. *The Guardian*.
- Kazemi, A., 2014. *Transparency Reporting for Beginners (RightsCon 2014)*. [video] Available at: <https://www.youtube.com/watch?v=QMyaV9yGpco&list=PLprTandRM960PUyig8SUxOViRicZztcFv&index=5> [Accessed 5 Jan. 2016].
- Kennedy, C.H. & Swire, P.P., 2002. State wiretaps and electronic surveillance after September 11. *Hastings L.J.*, 54, p.971.
- Knox Everette, W., 2015. "The Fbi Has Not Been Here [Watch Very Closely for the Removal of this Sign]" Warrant Canaries and First Amendment Protection for Compelled Speech. *George Mason Law Review, Forthcoming*.
- Kopstein, J., 2013. Silicon Valley's Surveillance Cure-All: Transparency. *The New Yorker*. [online] Available at: <http://www.newyorker.com/tech/elements/silicon-valleys-surveillance-cure-all-transparency> [Accessed 7 Feb. 2016].
- Kulikova, A., 2013. The Importance of Being Transparent: Looking at the ICT Companies' Transparency Reports Through the Prism of the NSA Surveillance Leak. Available at SSRN 2429707.
- Kumar, P., 2016. *Ranking Digital Rights Findings on Transparency Reporting and Companies' Terms of Service Enforcement*. [online] Available at: <http://Ranking Digital Rights Findings on Transparency Reporting and Companies' Terms of Service Enforcement> [Accessed 8 Apr. 2016].
- Labowitz, S., 2016. Discussion on Transparency Reporting and the GNI.
- Laidlaw, E.B., 2015. *Regulating speech in cyberspace: Gatekeepers, human rights and corporate responsibility*. Cambridge University Press.
- Landau, S., 2011. Where Have All the Wiretap Reports Gone? [Blog] *The Huffington Post*. Available at: http://www.huffingtonpost.com/susan-landau/wiretapping-laws_b_890498.html [Accessed 10 Jan. 2016].
- Lee, B., 2014. Taking the fight for #transparency to court. [Blog] *Twitter Blog*. Available at: <https://blog.twitter.com/2014/taking-the-fight-for-transparency-to-court> [Accessed 2 Apr. 2016].

- Losey, J., 2015. Surveillance of Communications : A Legitimization Crisis and the Need for Transparency. , 9, pp.3450–3459.
- MacKinnon, R., 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. Basic Books.
- MacKinnon, R., 2014c. *Ranking Digital Rights: Holding tech companies accountable on freedom of expression and privacy*. [online] Newschallenge.org. Available at: <https://www.newschallenge.org/challenge/2014/submissions/ranking-digital-rights-holding-tech-companies-accountable-for-respecting-and-protecting-internet-users-freedom-of-expression-and-privacy> [Accessed 8 Apr. 2016].
- MacKinnon, R. & McGlinchey, L., 2016. MacKinnon, R. (2016). Are tech companies doing enough to protect customer rights and privacy?. *Ford Foundation*.
- MacKinnon, R., & Magistad, M.K., 2016. Who's messing with your Internet rights? And who'd tell you if they did? *PRI*.
- Maclay, C.M., 2010. Protecting privacy and expression online: Can the Global Network Initiative embrace the character of the net. *Access controlled: The shaping of power, rights, and rule in cyberspace*, pp.87-108.
- Malcolm, J., 2015. *Benchmarking ICT companies on digital rights (Friends of the IGF)*. [online] Available at: <http://friendsoftheigf.org/transcript/777>
- Manes, J., 2016. Online Service Providers and Surveillance Law Transparency. , 23, pp.343–358.
- Maréchal, N., 2015. COMPASS| Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate. *International Journal of Communication*, 9, p.10.
- Masiello, B., 2014. The Unbearable Trust of the Internet. In: K. Brennan, ed., *Making Global Institutions Work*, 1st ed. Routledge.
- Microsoft, 2014. *Law Enforcement Requests Report*. [online] Available at: <https://www.microsoft.com/about/csr/transparencyhub/lerr/> [Accessed 6 Feb. 2016].
- Microsoft v. Lynch* [2016] (UNITED STATES DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT SEATTLE). Available at: <http://online.wsj.com/public/resources/documents/microsoftcomplaint.pdf>
- Miller, C., 2010. Google Reports on Government Requests and Censorship. [Blog] *The New York Times Bits*. Available at:

- http://bits.blogs.nytimes.com/2010/09/21/google-reports-on-government-requests-and-censorship/?_r=0 [Accessed 8 Jan. 2016].
- Naughton, J., 2016. Your WhatsApp secrets are safe now. But Big Brother is still watching you.... *The Guardian*. [online] Available at: <http://www.theguardian.com/commentisfree/2016/apr/10/whatsapp-encryption-billion-users-data-security> [Accessed 24 Apr. 2016].
- Necessary and Proportionate, 2013. *About the Principles*. [online] Available at: <https://en.necessaryandproportionate.org/about> [Accessed 2 Apr. 2016].
- Owsley, B.L., 2014. To Unseal or Not to Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders. *Calif. L. Rev. Circuit*, 5, pp.259-408.
- Parsons, C.A., 2015. Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports. *Evaluating the Effectiveness of Telecommunications Transparency Reports (January 6, 2015)*.
- Pegoraro, R., 2015. Tech Firms Trust Our Government Even Less Than You Do. *Yahoo! Tech*. [online] Available at: <https://www.yahoo.com/tech/tech-firms-trust-our-government-even-less-than-you-122203798219.html> [Accessed 8 Feb. 2016].
- Peterson, A. (2014). Here's why tech companies' NSA 'transparency reports' are mostly a PR stunt. *The Washington Post*. [online] Available at: <https://www.washingtonpost.com/blogs/the-switch/wp/2014/01/28/heres-why-tech-companies-nsa-transparency-reports-are-mostly-a-pr-stunt> [Accessed 8 Apr. 2016].
- Posner, M. & Labowitz, S., 2016. Why We're Leaving the Global Network Initiative. [Blog] *NYU Stern Center for Business and Human Rights*. Available at: <http://bhr.stern.nyu.edu/blogs/why-were-leaving-the-gni> [Accessed 8 Mar. 2016].
- Ranking Digital Rights., 2015. *2015 Indicators - Ranking Digital Rights*. [online] Available at: <https://rankingdigitalrights.org/index2015/> [Accessed 8 Jan. 2016].
- Reform Government Surveillance, 2013. *Reform Government Surveillance*. [online] Available at: <https://www.reformgovernmentsurveillance.com/USAFreedomAct> [Accessed 2 Apr. 2016].
- Roberts, J., 2014. *Gigaom | Apple's "warrant canary" disappears, suggesting new Patriot Act demands*. [online] Gigaom.com. Available at:

- <https://gigaom.com/2014/09/18/apples-warrant-canary-disappears-suggesting-new-patriot-act-demands/> [Accessed 7 Mar. 2016].
- Rodriguez, K., 2015. New Report Rates Peruvian ISPs: Who Defends Your Data?. [Blog] *EFF Deeplinks Blog*. Available at: <https://www.eff.org/deeplinks/2015/11/new-report-shows-which-peruvian-isps-care-about-their-users-privacy> [Accessed 8 Feb. 2016].
- Samway, M., 2014. *2014 Learning Forum on Transparency and Human Rights in the Digital Age - California*. [online] Telecommunications Industry Dialogue. Available at: <https://www.telecomindustrydialogue.org/2014-learning-forum-on-transparency-and-human-rights-in-the-digital-age-california-2/> [Accessed 7 Feb. 2016].
- Samway, M.A., 2014b. Internet, Human Rights, and the Private Sector, *The Geo. J. Int'l Aff.*, 15, p.25.
- Samway, M., 2016. companies in the information and communications technology industry respect human rights?. In: D. Baumann-Pauly and J. Nolan, ed., *Business and Human Rights: From Principles to Practice*, 1st ed. New York: Routledge, pp.136-147.
- Schneier, B., 2015. *Data and Goliath: the hidden battles to capture your data and control your world*, New York: W.W. Norton.
- Schwartz, P.M., 2008. Reviving Telecommunications Surveillance Law. *University of Chicago Law Review*, 75.
- Schwartz, P.M., 2002. German and US Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance. *Hastings LJ* 54, 751.
- Shelton, M., 2014. *Where the U.S. wiretap hotspots are*. Pew Research Center - Fact Tank. [online] Available at: <http://www.pewresearch.org/fact-tank/2014/07/14/where-the-u-s-wiretap-hotspots-are/> [Accessed 7 Feb. 2016].
- Shih, G. and Rigby, B. 2013. U.S. tech firms push for government transparency on security. *Reuters*. [online] Available at: <http://www.reuters.com/article/us-google-nsa-transparency-request-idUSBRE95A11820130612> [Accessed 2 Apr. 2016].
- Silk Transparency Reports Database., 2013. *Transparency Reports Database*. [online] Available at: <https://transparency-reports.silk.co/> [Accessed 8 Jan. 2016].

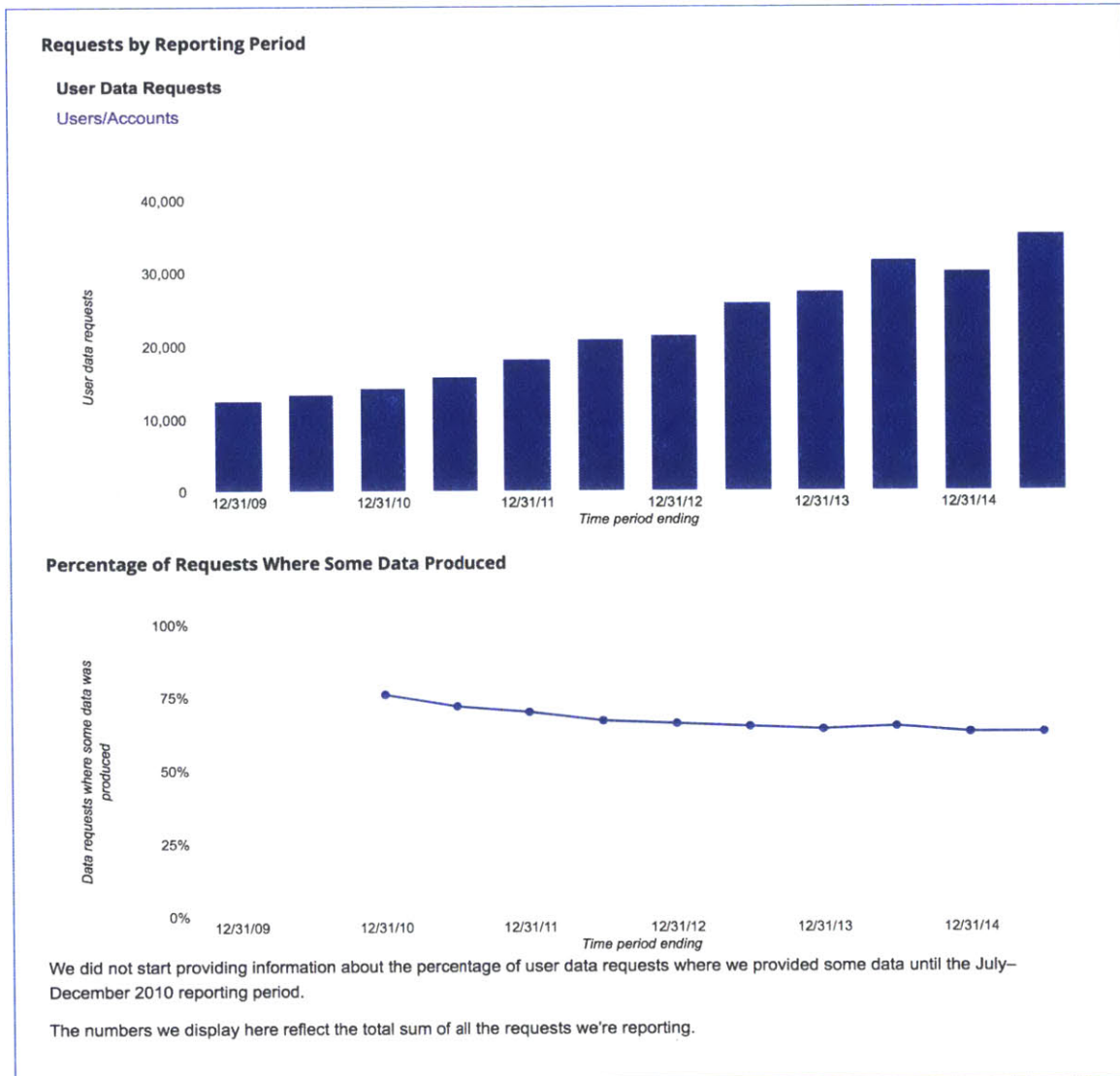
- Slater, D., 2006. EFF Urges Reversal of FCC's Forcing Internet Services To Be Wiretap-Friendly. [Blog] *EFF Deeplinks Blog*. Available at: <https://www.eff.org/deeplinks/2006/05/eff-urges-reversal-fccs-forcing-internet-services-be-wiretap-friendly> [Accessed 7 Feb. 2016].
- Soghoian, C., 2010. An end to privacy theater: Exposing and discouraging corporate disclosure of user data to the government. *Minnesota Journal of Law, Science & Technology*, *Forthcoming*.
- Soghoian, C., 2011. The Law Enforcement Surveillance Reporting Gap. Available at SSRN 1806628.
- Soghoian, C., 2012. *The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance* (Doctoral dissertation, Indiana University).
- Sprint, 2014. *Sprint Corporation Transparency Report*. [online] Available at: <http://goodworks.sprint.com/content/1022/files/CR%20Transparency%20Report%20Final%20version.pdf> [Accessed 8 Apr. 2016].
- Sullivan, D., 2013. *How To Bring More Transparency To U.S. Surveillance Programs*. [online] ThinkProgress. Available at: <http://thinkprogress.org/security/2013/07/03/2253791/transparency-surveillance-programs/> [Accessed 7 Feb. 2016].
- Sullivan, D., 2015. UN FORUM SERIES – Competition, Collaboration, and Corporate Accountability Rankings. [Blog] *The London School of Economics and Political Science - Measuring Business and Human Rights*. Available at: <http://blogs.lse.ac.uk/businesshumanrights/2015/12/01/un-forum-series-competition-collaboration-and-corporate-accountability-rankings> [Accessed 8 Feb. 2016].
- Terzian, D., 2013. The Fifth Amendment, Encryption, and the Forgotten State Interest. *Encryption, and the Forgotten State Interest*.
- Thielman, S., 2015. 'If this was a test, nearly everyone failed': how tech giants deny your digital rights. *The Guardian*. [online] Available at: <https://www.theguardian.com/technology/2015/nov/03/ranking-digital-rights-project-data-protection> [Accessed 5 Mar. 2016].
- T-Mobile, 2014. *Transparency Report*. [online] Available at: <https://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf> [Accessed 8 Mar. 2016].

- Uber, 2016. *Transparency Report*. [online] Available at: <https://transparencyreport.uber.com/> [Accessed 1 May 2016].
- Tumblr, 2014. *Transparency Report*. [online] Available at: <https://www.tumblr.com/transparency> [Accessed 6 Feb. 2016].
- Tuppen, C., 2013. *Opening the Lines A Call for Transparency from Governments and Telecommunications Companies*. [online] Global Network Initiative. Available at: http://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf [Accessed 3 Jan. 2016].
- Twitter, 2015. *Transparency Report*. [online] Available at: <https://transparency.twitter.com/country/us> [Accessed 6 March. 2016].
- UNESCO, 2014. *Fostering Freedom Online. The Role of Internet Intermediaries*, Available at: <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.
- United States Courts, 2015. *Wiretap Report 2014*. Wiretap Reports. [online] Available at: <http://www.uscourts.gov/statistics-reports/wiretap-report-2014> [Accessed 1 Nov. 2015].
- United States Courts, 2014. *Wiretap Report 2013*. Wiretap Reports. [online] Available at: <http://www.uscourts.gov/statistics-reports/wiretap-report-2013> [Accessed 1 Nov. 2015].
- United States Courts, 2013. *Wiretap Report 2012*. Wiretap Reports. [online] Available at: <http://www.uscourts.gov/statistics-reports/wiretap-report-2012> [Accessed 1 Nov. 2015].
- United States Courts, 2012. *Wiretap Report 2011*. Wiretap Reports. [online] Available at: <http://www.uscourts.gov/statistics-reports/wiretap-report-2011> [Accessed 1 Nov. 2015].
- United States Courts, 1969. *Wiretap Report 1968 Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications*. [online] Available at <http://www.heinonline.org/HOL/Page?handle=hein.usfed/wirtp1968&size=2&collection=usfed&id=3>
- Verizon, 2014. *United States Report*. Transparency Report. [online] Available at: <http://www.verizon.com/about/portal/transparency-report/us-report/> [Accessed 8 Apr. 2016].

- Wexler, R., 2014. Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders. *The Yale Law Journal Forum*, 124, pp.158–179. Available at: <http://www.yalelawjournal.org/forum/warrant-canaries-and-disclosure-by-design>.
- Woolery, L., Budish, R. & Bankston, K., 2016. *Transparency Reporting Toolk: Survey & Best Practice Memos for Reporting on US Government Requests for User Information*, Available at: https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Transparency.pdf.
- Wright, P., 2015. *Benchmarking ICT companies on digital rights Workshop (Internet Governance Forum)*. [online] Available at: <http://www.intgovforum.org/cms/187-igf-2015/transcripts-igf-2015/3005-2015-11-11-ws-60-benchmarking-ict-companies-on-digital-rights-workshop-room-7-finished>
- Yahoo, 2015. Ranking Digital Rights Releases Corporate Accountability Index. [Blog] *Yahoo Business & Human Rights Program*. Available at: <https://yahoobhrp.tumblr.com/post/132476359684/ranking-digital-rights-releases-corporate> [Accessed 8 Feb. 2016].

Appendix A

Screenshots from Google's Transparency Report



Non-content requests

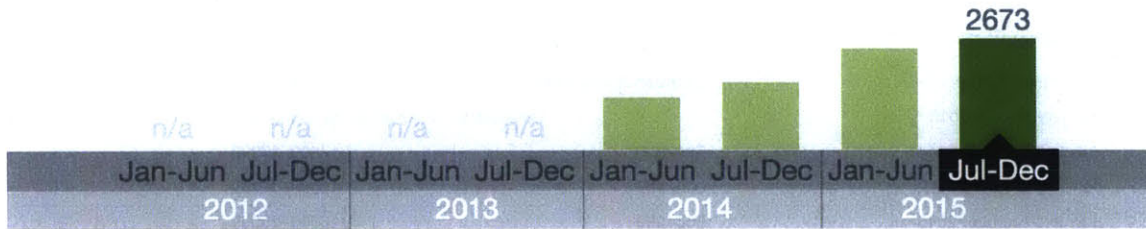
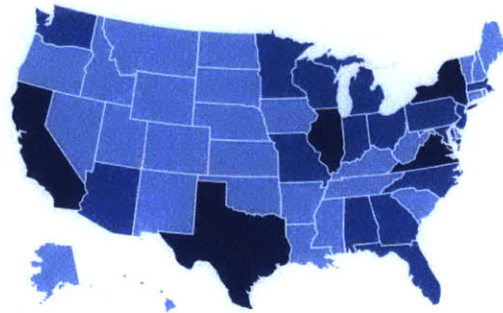
Reporting Period	Number of requests	Users/Accounts
January to June 2015		Data subject to six month reporting delay
July to December 2014	0-499	0-499
January to June 2014	0-499	0-499
July to December 2013	0-499	0-499
January to June 2013	0-499	0-499
July to December 2012	0-499	0-499
January to June 2012	0-499	0-499
July to December 2011	0-499	0-499
January to June 2011	0-499	500-999
July to December 2010	0-499	500-999
January to June 2010	0-499	0-499
July to December 2009	0-499	0-499
January to June 2009	0-499	0-499

Content requests

Reporting Period	Number of requests	Users/Accounts
January to June 2015		Data subject to six month reporting delay
July to December 2014	500-999	17500-17999
January to June 2014	500-999	15000-15499
July to December 2013	500-999	15500-15999
January to June 2013	500-999	9500-9999
July to December 2012	500-999	12500-12999
January to June 2012	500-999	8000-8499
July to December 2011	500-999	9500-9999
January to June 2011	500-999	7000-7499
July to December 2010	0-499	5000-5499
January to June 2010	0-499	3500-3999
July to December 2009	0-499	3500-3999
January to June 2009	0-499	2000-2499

Screenshot from Twitter's Transparency Report

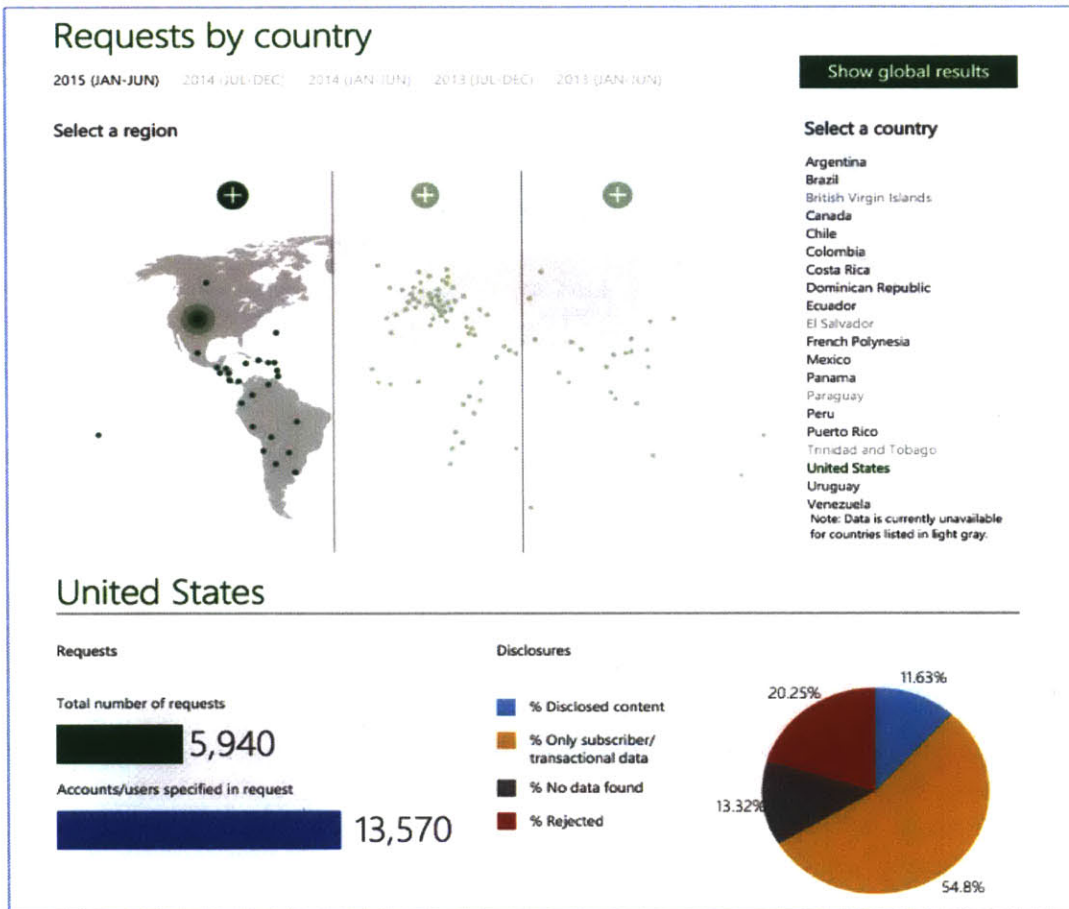
United States



Breakdown by state / territory (2015: Jul - Dec):


- Alabama (26)
- Alaska (9)
- Arizona (43)
- Arkansas (6)
- California (313)
- Louisiana (10)
- Maine (2)
- Maryland (62)
- Massachusetts (57)
- Michigan (50)
- Oklahoma (5)
- Oregon (3)
- Pennsylvania (60)
- Puerto Rico (13)
- Rhode Island (1)

Screenshot from Microsoft's Transparency Report



Appendix B

The "Who Defends Your Data?" Report Evaluating ISPs in Peru




	Política de Privacidad	Autorización judicial	Notificación a usuarios	Reportes de transparencia	Compromiso con la privacidad
BITEL	★	★	★	★	★
CLARO	★	★	★	★	★
ENTEL	★	★	★	★	★
MOVISTAR	★	★	★	★	★
OLO	★	★	★	★	★

HIPERDERECHO.ORG/QDTD

Results from Peruvian ISPs' privacy protections

The "Who Defends Your Data?" Report Evaluating ISPs in Mexico

THE RESULTS

	Política de privacidad adecuada	Exige autorización judicial	Notifica a usuarios	Publica informe de transparencia	Defiende usuarios en tribunales	Compromiso con privacidad	Final
AXtel 		★				★	★★★★★
Cablemás		★				★	★★★★★
USACEL		★		★	★	★	★★★★★
.iZZI!		★				★	★★★★★
MEGACABLE		★					★★★★★
movistar		★		★		★	★★★★★
nextel		★		★		★	★★★★★
TELMEX. / telcel		★		★	★	★	★★★★★