
DIGITAL ACCESS TO SCHOLARSHIP AT HARVARD
DASH.HARVARD.EDU

HARVARD LIBRARY


The Transparency Reporting Toolkit: Reporting Guide and Template for Reporting U.S. Government Requests for User Information

Citation

Woolery, Liz, Ryan Budish, Kevin Bankston 2016. The Transparency Reporting Toolkit: Reporting Guide and Template for Reporting U.S. Government Requests for User Information. Berkman Klein Center for Internet & Society Research Publication.

Link

http://nrs.harvard.edu/urn-3:HUL.InstRepos:29914191

Terms of use

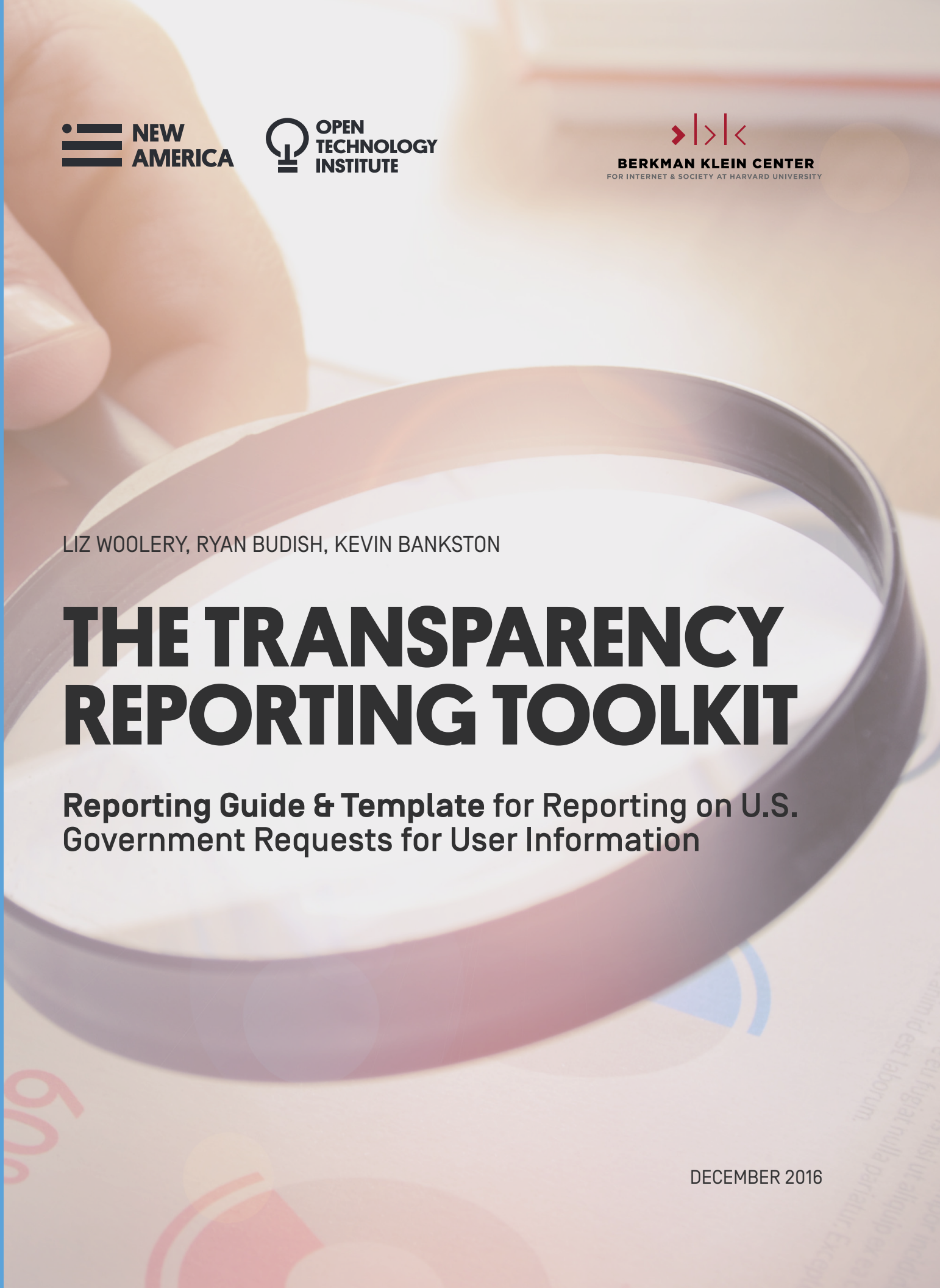
This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material (LAA), as set forth at
https://harvardwiki.atlassian.net/wiki/external/NGY5NDE4ZjgzNTc5NDQzMGIzZWZhMGFlOWI2M2EwYTg

Accessibility

https://accessibility.huit.harvard.edu/digital-accessibility-policy

Share Your Story

The Harvard community has made this article openly available.
Please share how this access benefits you. Submit a story



NEW AMERICA

OPEN TECHNOLOGY INSTITUTE

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

LIZ WOOLERY, RYAN BUDISH, KEVIN BANKSTON

THE TRANSPARENCY REPORTING TOOLKIT

Reporting Guide & Template for Reporting on U.S. Government Requests for User Information

DECEMBER 2016

Report © 2016 NEW AMERICA and THE BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY

This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of this content when proper attribution is provided. This means you are free to share and adapt this work, or include our content in derivative works, under the following conditions:

- **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit creativecommons.org.

If you have any questions about citing or reusing New America content, please visit www.newamerica.org. If you have questions about citing or reusing Berkman Klein Center content, please visit https://cyber.law.harvard.edu.

All photos in this report are supplied by, and licensed to, **Shutterstock.com** unless otherwise stated.

AUTHORS

Kevin Bankston, Director, Open Technology Institute, bankston@opentechinstitute.org
Ryan Budish, Senior Researcher, Berkman Klein Center for Internet & Society, rbudish@cyber.harvard.edu
Liz Woolery, Senior Policy Analyst, Open Technology Institute, lizwoolery@opentechinstitute.org

ACKNOWLEDGMENTS

The *Transparency Reporting Toolkit* would not have been possible without insight and help from Dorothy Chou, Christian Dawson, Jeremy Kessel, Rob Faris, Urs Gasser, Robyn Greene, Jess Hemerly, Priya Kumar, Colin Maclay, Eric Sears, Alison Yost, OTI Open Web Fellow Gemma Barrett, members of the i2C Coalition, and the many others who have contributed to this report by offering time, thoughts, and insights throughout this process. This work has been generously supported by the MacArthur Foundation.

ABOUT THE OPEN TECHNOLOGY INSTITUTE

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

ABOUT THE BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

Founded in 1997, the Berkman Klein Center for Internet & Society at Harvard University is dedicated to exploring, understanding, and shaping the development of the digitally-networked environment. A diverse, interdisciplinary community of scholars, practitioners, technologists, policy experts, and advocates, we seek to tackle the most important challenges of the digital age while keeping a focus on tangible real-world impact in the public interest. Our faculty, fellows, staff and affiliates conduct research, build tools and platforms, educate others, form bridges and facilitate dialogue across and among diverse communities.







BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

WITH GENEROUS SUPPORT FROM
MacArthur Foundation

TABLE OF CONTENTS

PREFACE **1**

Introduction 2

Understanding Transparency Reporting 4

TRANSPARENCY REPORTING GUIDE **9**

Requests from U.S. Government and Law Enforcement Entities *11*

Granularity of Reporting 12

Additional Considerations for Legal Process Reporting 15

Counting Requests 18

Responding to Requests 21

National Security Orders *25*

Picking a Reporting Structure for National Security Orders 26

Reporting NSLs & FISA Orders Under the USA FREEDOM Act 30

Requests from Foreign Governments and Law Enforcement Entities *33*

Outside the U.S.: Prospective & Retrospective Requests 34

Other Reporting Practices to Consider *37*

Non-Counting & Qualitative Features 38

Uncommon Best Practices & Other Notable Ideas 40

TRANSPARENCY REPORTING TEMPLATE **41**

PREFACE

INTRODUCTION

ABOUT THE *TRANSPARENCY REPORTING TOOLKIT*

The *Transparency Reporting Toolkit* is a joint project by New America's Open Technology Institute and Harvard University's Berkman Klein Center for Internet & Society. The purpose of the *Toolkit* is to make it easier for companies to create better transparency reports about government requests for user data. Similarly, by providing a template and best practices, the *Toolkit* aims to make it easier for new companies to begin transparency reporting. By following the recommendations in this guide, which are grounded in existing best practices, transparency reports can become more consistent, easier to understand, and more effective.

This guide is one part of our ongoing *Transparency Reporting Toolkit* project, which currently includes:

- The **Survey & Best Practice Memos**—A survey of 43 transparency reports, identifying best practices across eight different areas (March 2016)
- This **Reporting Guide & Template**—This guide provides a practical starting point for companies that want to create or improve their transparency reports, including a model transparency reporting template for companies designing their first report (December 2016)

These components of the *Toolkit* build on our extensive research into transparency reporting. For the past three years we have surveyed transparency reports, hosted multiple workshops with representatives from academia, civil society, and a variety of internet companies, and conducted numerous interviews with transparency reporting leaders at many internet and technology companies. From this research we have identified the best practices and recommendations that are central to this *Toolkit*.

ABOUT THE REPORTING GUIDE & TEMPLATE

Through all of our conversations, it became clear that a wide variety of companies, those both big and small, wanted tools that could help them more easily create transparency reports that followed consensus best practices. This guide assumes familiarity with our eight-part *Transparency Reporting Toolkit Survey & Research Memos*, released in March 2016, which identifies best practices in reporting based on an extensive survey of current practices. This reporting guide and template is an extension of that work and provides practical assistance to help companies translate those best practices into their reports.

This guide is not legal advice. The best practices described here are largely based on practices observed throughout a range of existing reports. However, each company's circumstances, market positioning, data collection, business models, and risks are different, and the decisions of when and how to produce a transparency report should be based on those unique factors. This guide can be a resource for companies as they work with their lawyers in responding to and reporting on government requests for user data.

LOOKING AHEAD

Transparency reports are still in their infancy. In the years since Google released its first transparency report in 2010, we've seen an explosion in both the number and diversity of reports. We fully expect the experimentation with reporting approaches and styles to continue over the coming years. Our work has focused on one small part of the transparency landscape: reporting on government requests for user data, which has been a nearly universal element in transparency reports. Some companies have developed, or are developing, transparency reports that cover a wide range of other equally important areas, including content takedowns, copyright takedowns, terms of service violations, and much more.

For that reason, this is a work in progress. This work reflects our understanding of best practices today; as companies continue to iterate, best practices will evolve and change. For example, many individuals across companies, civil society, and academia are currently trying to identify the best approaches for transparency with respect to company responses to terms of service violations. As transparency reports develop, we hope to revisit these resources and update them. Along the way, **we welcome feedback**. Our research has documented such a vast array of approaches and practices within the landscape of current transparency reports that it is impossible for us to address all questions or resolve all tensions, and we invite feedback from those who think we have missed something.

We hope this template and guide helps companies as they seek to develop their transparency reports, and we look forward to working with them in further developing this resource. As companies work to implement this guidance, we encourage them to contact us to share feedback and update us on changes to their reports. Feedback and other comments can be sent to transparency_toolkit@cyber.harvard.edu.

—Kevin Bankston, Ryan Budish, and Liz Woolery

Scope of the *Transparency Reporting Toolkit*'s *Reporting Guide & Template*

Having surveyed the landscape of transparency reporting and identified best practices, we set out to translate that research into a the *Transparency Reporting Toolkit's Reporting Guide & Template*. This document walks companies through reporting using best practices by doing the following:

- Exploring the hows and whys of reporting
- Identifying best practices
- Explaining why each practice was selected
- Highlighting innovative practices companies might consider adopting

This document reflects input from a wide variety of individuals and is intended to be a resource for companies as they consider how to create transparency reports and incorporate best practices into their own reports.

UNDERSTANDING TRANSPARENCY REPORTING

TYPES OF TRANSPARENCY REPORTS

Companies are publishing a wide and ever-growing range of non-financial reports. These reports cover topics such as climate change, supply chain labor standards, diversity, copyright takedown notices, and government censorship. The focus of this guide is transparency reporting on government requests for user data. These government requests are specific legal processes that courts, law enforcement agencies, and intelligence agencies can issue to demand data from companies. These processes, such as warrants and subpoenas, can come from a range of authorities operating at the federal, state, and local levels, as well as international government agencies. Government requests can also come from regulatory agencies conducting civil (rather than criminal) investigations. Reporting on these demands for user data is important, but it is important to remember that it is just one of many kinds of transparency reporting. Each company, depending on their own unique circumstances, should consider the full range of transparency reporting. This is not an all-or-nothing endeavor—each kind of transparency reporting can be additive. Companies adopting the mechanisms and processes necessary to produce one kind of transparency report will lower the barriers to producing others.

RECEIVING & RESPONDING TO REQUESTS FOR USER DATA

Transparency reports about requests for user data are an increasingly important way that internet and telecommunications companies are communicating with their users and others about practices that can affect user privacy and security. For that reason, the first step in transparency reporting happens well before a company publishes a report. Instead, the first step comes when companies develop, test, and implement policies for receiving, processing, and fairly and consistently responding to all valid and lawful requests for user information.

Law enforcement and intelligence agencies have realized the immense value of the data that internet and telecommunications companies collect and store. As a result it has now become common investigatory practice for law enforcement to request data from the services that a target may have used. If a company collects and stores data, receiving a government request has become a matter of "when," not "if." It is crucial for all companies, even those that have not yet received government requests, to expect and plan for these requests.

Developing a plan for handling government requests is both critical and challenging. There is no substitute for consulting with legal counsel. Only a lawyer can help a company identify lawful requests and develop effective compliance mechanisms. Based on our conversations with companies, we have identified a few broad considerations that companies should discuss with their lawyers:

- *Tracking Requests*: When requests arrive, it is important for companies to have a process in place to keep

track of requests and their status. In our interviews with companies we learned that prior to producing a transparency report, some had tracked requests using a shared e-mail inbox while others let each local office handle requests separately. While such approaches can work, particularly for small companies with few requests, they increase the risk of mistakes or inconsistent handling requests. Instead, companies should use a single, centralized process for tracking, tagging, and keeping tabs on requests from the moment they are received until the time a response is provided to the government.

- *Classifying Requests*: Before a company can respond to a request, it must be able to properly identify the type of process and the agency or court that issued it. Just because a request says "warrant" at the top of the page does not make it so. Companies have told us about receiving requests that are inaccurately labeled (either intentionally or mistakenly). The type of process can be determinative of the kinds of information that a company can or must disclose. For example, many companies will only disclose user content in response to a warrant. For that reason, it is important that companies have trained staff that can look past the title to properly classify the request.
- *Responding to Requests*: The moment a request is received is not the time for a company to try to determine the kinds of data they keep, which of that data is user content, and whether the legal process is sufficient for the requested data. Particularly for companies that do not receive many government requests, receiving a request can be scary or confusing—feelings that can be amplified when government agencies claim it is an emergency. For that reason, companies should work with their legal counsel to develop a playbook for responding to requests before they receive them.
- *Providing User Notice*: Government requests are increasingly accompanied by a gag order that prevents companies from informing the target of the investigation. For those requests without gag orders, companies must decide whether and under what circumstances they'll provide notice to their users. For requests with gag orders, companies must decide whether to challenge the order and/or to inform users after the gag order has lifted. Companies will also need to identify processes for contacting users.
- *Keeping Data Secure*: Information about law enforcement and intelligence requests is sensitive information in itself. In order to keep this information secure, companies should carefully consider how this data is maintained and who has access to it.

CREATING A TRANSPARENCY REPORT

There are many reasons why a company might decide to produce a transparency report. These reasons can include:

- Signaling company values
- Easing fears about privacy
- Raising awareness about the scale and scope of government requests
- Educating lawmakers
- Advocating for policy change
- Improving company morale
- Competing with peer companies

Good reasons for creating a report, however, are often not sufficient to convince companies to create transparency reports. After all, the creation of reports requires time and money that could otherwise be spent developing new products and services. Moreover there is a widely held fear that publishing a transparency report will lead to an influx of government requests. In almost every company that we have talked to there was a champion behind the initial report—someone who believed strongly in transparency and who could make the case within the company that the benefits would outweigh the costs. It is our hope that this guide will enable individuals within companies to advocate for the value of transparency reporting.

Advocating for transparency reporting early on can help ensure that processes for receiving, tracking, and responding to government requests are in place well before the company produces its first report. Creating a transparency report can be relatively easy when a company has already been tracking the relevant data, but this requires establishing the processes for receiving, tracking, and responding to government requests with an eye toward transparency reporting. In that way, planning for a transparency report can help inform and shape company processes for tracking and responding to requests. For example, by considering the following issues well before creating their first report, companies can lay the groundwork for reporting, improve their own processes, and make the eventual production of a report much easier. These issues include:

- How they define the "content" of communications versus "non-content" data
- When they ask law enforcement to refine or change its requests
- The kind of information they can and will produce for certain types of legal process

Producing a transparency report requires clear and consistent recording of data. Companies must identify the kinds of information they want to include in their report well before they create their first transparency report so that they can begin tracking that information. A range of data can be tracked, including:

- Requesting agency
- Type of request
- Type of data requested
- How the company responded
- When the company responded
- When the company notified the subject of the request
- Number of accounts affected by the request

In our conversations with companies we've learned that the process of creating a transparency report can be a great opportunity for companies to, in collaboration with counsel, refine and improve their processes for responding to government requests. Several companies described the unexpected benefits of consistency, accuracy, and organization that came from the process of crafting their first transparency report. Before they could confidently tell the public the number of requests they had received and responded to, they had to standardize policies, centralize how they tracked requests, establish internal guidelines and quality control systems and more.

Similarly, we've learned that transparency reporting is an iterative and evolutionary process. In the course of working on this guide, we've seen several companies revise and update their reports, incorporating feedback, and implementing best practices. No company should let perfect be the enemy of the good when it comes to producing a transparency report. Even companies that have been producing reports for years are still experimenting with new formats and approaches.

This template and reporting guide helps companies think through each of these, as well as other parts of transparency reporting. In particular, this template and reporting guide looks at five major elements of transparency reports, and offers guidance on how companies can approach each one. These five areas are:

- How to report on the number and kind of legal process requests—which types of processes to count, and the granularity for each type of process.
- How to count legal process requests—when to count one-time/retrospective versus prospective requests, and how to count the number of responsive requests.
- How to describe the outcomes of requests—what types of outcomes to report, how to define different types of compliance with requests, and when and how to describe user notice.
- How to count national security orders—how to apply the various reporting options available under the USA FREEDOM Act.
- How to utilize the qualitative features of reports—how to describe company policies and procedures, when and how to publish reports, and how to make reports more accessible and understandable.

The guide and template describe a variety of best practices, and we hope companies will adopt many of them. If there is one practice, however, that we strongly urge every company to adopt, it is this: **no matter what you do, be clear about what you are reporting on**. More than anything else, the current generation of transparency reports suffer from a lack of clarity about how they are arriving at the numbers they are reporting. While we've been privileged to probe companies on their practices, transparency reports should not require access to the report authors in order to understand them. While the best practices described in the rest of this guide are useful for improving the consistency and quality of reports, the value of reporting would increase immensely with only the addition of greater clarity into company practices.

ADDITIONAL RESOURCES

This reporting guide and template aims to help companies understand the critical components of transparency reporting and implement the best practices for each one. It is one resource that can help companies create (or improve) their transparency reports. Other resources that might be helpful include:

- For more information about government requests for data and other government demands: *Managing Users' Rights Responsibly: A Guide for Early Stage Companies*, The Berkman Klein Center for Internet & Society and the law firm of Foley Hoag, http://www.csrandthelaw.com/wp-content/uploads/sites/2/2016/03/Managing-Users-Rights-Responsibly_A-Guide-For-Early-Stage-Companies-no-logos.pdf
- For assistance finding legal counsel: The Electronic Frontier Foundation (EFF) is a user rights-focused non-profit that can provide or locate appropriate legal services, https://www.eff.org/pages/legal-assistance
- For examples of a broad range of legal demands for user data, see the sample documents in the Appendix of the 2009 edition of *Searching and Seizing Computers and Obtaining Electronic Evidence in*

Criminal Investigations, a guide published by the Justice Department's Computer Crime and Intellectual Property Section (CCIPS), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

- For examples of National Security Letters, see these examples provided by Google and Yahoo, https://googleblog.blogspot.com/2015/05/new-data-more-facts-update-to.html, https://blog.google/topics/public-policy/sharing-national-security-letters-public, and https://yahoopolicy.tumblr.com/post/145258843473/yahoo-announces-public-disclosure-of-national
- For more information about government requests for sharing economy companies: EFF's *Who Has Your Back?*, https://www.eff.org/who-has-your-back-2016
- For an index of transparency reports: Access Now's Transparency Reporting Index, https://www.accessnow.org/transparency-reporting-index/
- For a ranking of internet and telecommunications company practices on a range of digital rights issues: *Ranking Digital Rights Corporate Accountability Index*, https://rankingdigitalrights.org

TRANSPARENCY REPORTING GUIDE

REQUESTS FROM U.S. GOVERNMENT AND LAW ENFORCEMENT ENTITIES

GRANULARITY OF REPORTING

This approach is based on the way that several companies report on different legal processes in their transparency reports, as highlighted in Memo #1 of our *Transparency Reporting Toolkit's Survey & Research Memos*. There are a number of legal processes a company can receive requesting access to a user's information. For detailed explanations about these processes, see the glossary at the end of this document.

RECOMMENDED APPROACH

An ideal report will provide the number of government requests acted on (e.g., rejected or responded to), for each of the following individual legal processes every six months:

- Search Warrants
- Wiretap Orders
- Other Court Orders
- Criminal Subpoenas
- Civil Subpoenas (from government investigations)
- Pen Register/Trap and Trace Orders
- Emergency Requests

TYPES OF LEGAL PROCESSES RECEIVED

	Search Warrants	Wiretap Orders	Pen Register / Trap and Trace Orders	Other Court Orders	Subpoenas		Emergency Requests	TOTAL
					Criminal	*Civil*		
# Received [1]								

[1] *Total number of orders of any kind acted on (e.g., rejected or responded to) during [TIME PERIOD].*

Aggregate Data

In addition to reporting the number of each type of process received, most companies report—and we recommend that they report—certain aggregate numbers to attempt to reflect the larger scope and impact of the requests.

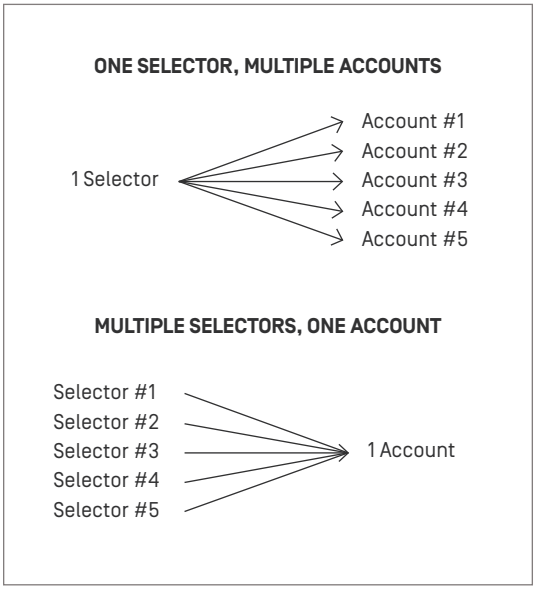
The two most common types of aggregate numbers we have seen are totals reflecting:

1. The **number of selectors specified in all requests received**. A selector is essentially the search term that the government is asking the company to look for in responding to the request. For example, it might be a name, a phone number, an IP address, an e-mail address, or any unique identifier that allows a company to locate responsive data. A government request might include a single selector or

it might include many. Multiple selectors might relate to a single account (e.g., many e-mail aliases for a single account) or a single selector might relate to many accounts (e.g., many users on the same IP address).

Why Selectors?

We strongly recommend that all companies count and report on selectors both because it is the clearer and more objective way of counting, and also because it is unclear how companies are currently calculating (or defining) "accounts affected." In addition, reporting on the number of selectors requested, in combination with other numbers, is a useful data point—this way, the average number of selectors per request and the average number of accounts per selector can be determined. Reporting on the number of total selectors does not require the company to conduct a forensic investigation and count the number of accounts; companies need only count the number of selectors listed in each piece of legal process.



2. The **number of accounts potentially affected by all requests received**. This is the number of accounts that would be affected if all of the requests were complied with.

Accounts Potentially Affected

However, if a company wants to additionally try to reflect the number of accounts potentially affected by all of the requests, there is one simple method we've learned of in our interviews with companies that we would recommend: add the total number of accounts actually affected by the requests in which data was handed over and the total number of selectors in all remaining requests that were not responded to. As with all of our recommendations, regardless of the method a company chooses, they should clearly explain that approach in their transparency report.

SELECTORS & ACCOUNTS FOR ALL OF THE ABOVE REQUESTS

Total # of Selectors Specified by All of the Above Requests	

Total # of Accounts Potentially Affected by All of the Above Requests	

Preservation Requests

We also encourage companies to report on requests to preserve evidence made under 18 U.S.C. § 2703(f). However, since these preservation requests do not involve a demand for nor disclosure of user data, they

should be reported separately from other legal processes.

PRESERVATION REQUESTS

# Received	# of Selectors Specified	# of Accounts Responsive

ADDITIONAL CONSIDERATIONS FOR LEGAL PROCESS REPORTING

Reporting on legal processes received is not always straightforward. The fractured approach to reporting now seen across different companies' transparency reports is evidence of this. To that end, there are several "definitional" issues that should be considered in advance of reporting and explained within the reports.

RECOMMENDED APPROACH

Subpoenas
We recommend that subpoenas reported include (and break out separately) both criminal and civil subpoenas, so long as they are from the government. For example, a subpoena from civil litigation between the company and an individual would not be included, but a subpoena from the Securities and Exchange Commission would be. No major companies currently report on civil subpoenas issued as part of non-governmental litigation, but we urge companies to consider tracking such information as it raises similar privacy concerns.

Other Court Orders
This refers to court-issued orders that are not warrants, wiretaps, or pen register/trap and trace orders. The most common of these orders will be orders authorized under 18 U.S.C. § 2703(d). In narratives accompanying their reports, companies should note if they've received any other kinds of court orders.

Emergency Requests
These are only emergency requests directly from the government. These are not reports to the National Center for Missing and Exploited Children, and not unsolicited voluntary disclosures. This does include verbal or in-person demands. All other emergency orders issued by a court (e.g., emergency pen register or emergency wiretap orders) should be counted within their specific legal process, and not as emergency requests.

MLAT (Mutual Legal Assistance Treaty)
We do not recommend counting MLAT requests—i.e., requests by the U.S. government on behalf of a foreign government—as a separate category because often companies will not know if a given request originated as an MLAT. Instead, the recommended practice is for companies to use the narrative portion of their report to explain the MLAT process and share any information it has about the requests that they believe originated through the MLAT process. One approach is to include the percentage of orders definitively known to have been issued through MLATs. For example, Twitter's report for the second half of 2015 notes that "8% of court orders and 1% of search warrants received have been explicitly identified as having been issued through MLAT procedures, coming from 12 different countries." The company also lists those countries.

All Writs Act Requests

Following the December 2015 San Bernardino shooting, the U.S. government attempted to use the All Writs Act to compel Apple to circumvent the encryption of an iPhone seized during the investigation. The All Writs Act is a federal law from 1789 under which courts can authorize orders ("writs") that compel a party to take a particular action. In response to the backlash that ensued, at least one company—Dropbox—added a note in its transparency report that the company "did not receive any orders issued under the authority of the United States All Writs Act of 1789." Should companies want to report on All Writs Act requests, we recommend following Dropbox's approach and including that information in a narrative portion of the report (as opposed to the section on demands for user data).

Preservation Requests

Because only a couple of companies currently report on preservation requests (either at the country or global levels), including it is not currently a best practice. However, we encourage additional companies to begin keeping track of the number of preservation requests and consider adding it to future transparency reports.

Listing All Requests

CREDO Mobile has taken the unusual approach of individually listing each request they have received, including type of request, requesting agency, user notice, and customer state. Because this practice has not been widely adopted, we do not recommend this for all companies. Moreover, for larger companies this would quickly become unmanageable. However, we suggest that companies with a smaller number of government requests consider taking the CREDO approach.

Reporting "0" Requests

Some company reports exclude legal processes they have not received. For example, a company may omit the "Wiretap Order" column if the company has received no wiretap requests. We advise against this and instead recommend including all legal processes and reporting "0" for those that have not been received. However, if a company chooses not to report on these processes at all, we recommend that they include a statement explaining that they have received no legal processes other than those reported.

Time Period of Reports

The consensus among current transparency reports is to release reports every six months. Six months is adequate time for the internal logistics of publishing a report, including new features and narratives to accompany the report, while also ensuring that the published data is not quickly out of date. Less than six months would limit the amount of preparation time, research, and writing that goes into a report. Greater than six months would result in data that may be many months (if not at least a year) old, and would also create challenges for identifying trends in the data.

With respect to timing, we recommend that companies publish their reports as soon as practicable. Ideally that would mean issuing a report once in January (covering July-December of the preceding year), and once in July (covering January-June of that year). However, the logistics of publishing an updated report can delay publication, so we instead recommend that companies publish as soon as they are able. A few companies have provided "live" transparency reports, constantly updating their reports as new requests come in. In order to ensure comparability across the industry, we recommend that companies

do this only if they also provide six-month summaries consistent with this guide. Reports should include the time period covered in a clear and obvious location. A date of publication should be included as well.

COUNTING REQUESTS

A surprisingly difficult aspect of creating a transparency report is counting. While the previous sections address which legal processes to count, this section deals with how to divide and classify the data being reported.

RECOMMENDED APPROACH

Terminology

Perhaps the most important recommendation in this entire guide is this: even if companies follow no other recommended practices, companies should be specific and clear in their transparency reports as to how they are defining the terms and what they are including in each category. This means being specific about what companies are counting and reporting on—whether it is accounts, users, devices, or e-mail addresses, for example. This is important for all transparency reports, but even more so for those that are taking an unconventional or non-best practice approach. For example, counting a variety of requests including emergency requests in a catchall category such as "Other Orders" is not a best practice, but if a company chooses to use that approach, it is incredibly confusing to readers unless that category is defined in a clear and accurate way.

Numbers vs. Percentages

Some companies include the number of each type of legal process received, others report what percentage of all requests a given process accounts for, and others include both numbers and percentages. The strong recommendation is that all companies include specific numbers for each type of legal process received. Percentages should be included, but only in addition to specific numbers. Moreover, we recommend that companies provide exact numbers (except where prohibited by law), and do not provide ranges or imprecise values (e.g., "<10").

One-Time and Retrospective Requests

The current consensus is that for one-time/retrospective requests, companies should count the request in the period in which they acted on the request (either rejected or responded to the request), not the period in which they received the request (if they did not respond or reject in the same period).

Renewals and Prospective Requests

No companies are currently explicit about how they are reporting renewed and prospective requests. However, based on conversations with stakeholders and experts, we suggest the following practice:

- Each renewal of an order counts as a new order.
- For wiretap orders (30-day duration) and pen register orders (60-day duration), we recommend counting at the moment the wiretap or pen register is set and recording begins. The vast majority of these orders will both begin and end in a single six-month reporting period. However, for those that

do not, companies would count the orders in the transparency report covering the period in which they were set, not when they concluded.

- Based on discussions with companies currently reporting, the most common practice is not to de-duplicate users/accounts impacted by renewed requests. Instead, these users/accounts should be counted again at the start of the renewed order.

Amended Requests

Consistent with our recommendations for renewals, we recommend that companies treat amended requests as new requests. When a company pushes back against a request for any reason (e.g., overbroad, incomplete, improper form) that would count as a rejection (see our section on outcome reporting below). If a law enforcement agency later amends the request to correct the defect, the amended request would be counted as a new request. This approach enables companies to prepare their reports without needing to wait to see if a rejected request is later amended. It also allows companies to include data that reflects the number of requests that are initially invalid or overbroad,

Combined Requests

One unresolved issue is how to handle the common situation where two types of legal process are combined within a single request. For example, pen register and 2703(d) orders are often issued in combination to obtain stored records of individual accounts identified by the pen register surveillance without the police having to go back to court for another order. Similarly, so-called "hybrid orders" combining 2703(d) orders with pen register orders are often used to obtain real-time cell phone location information that is not legally obtainable with a pen register alone. Some potential approaches for handling this situation are described below. We encourage companies to experiment and provide feedback on these approaches.

- *Option 1 (recommended): Count as one order and count in the most "invasive" category*
  Although most reports do not specify how companies handle combined requests, the most common approach, based on consultation with a range of companies, is to count the combined request as one request, and categorize that one request by its most "invasive" component. For example, prospective surveillance is traditionally considered more invasive than access to stored information, therefore a hybrid 2703(d)/pen register order would be counted as a single pen register order. The primary drawback of this approach is that it could be considered undercounting, which makes it all the more important to clearly and accurately report the number of accounts affected by the orders received.
- *Option 2: Count separately*
  Under this approach, companies count and categorize each aspect of the order individually, since they are under separate legal authorities and may be seeking distinct information. However, in those cases where the combined order is seeking a single category of information—e.g., hybrid orders for cell phone location information—this leads to double-counting. Again, this highlights the need to be clear and accurate regarding the number of accounts affected, regardless of the type or number of orders. Another drawback to this approach is that it requires staff responsible for the transparency report to look beyond the order in front of them and obtain more information about exactly how it is being used before being able to count it, adding to the complexity of the process.

Although Option 1 appears to be the most popular, as with many aspects of transparency reporting, the most important thing—regardless of which option companies choose—is to be very clear in the report about which method is used.

RESPONDING TO REQUESTS

Sharing the number and type of requests received by a company is an important part of building trust with users and customers. However, reporting on what happens after those requests are processed internally is equally important. Outcome and compliance data adds context and can demonstrate the company's commitment to protecting users by narrowing requests or by carefully reviewing requests.

RECOMMENDED APPROACH

Report Outcomes on a Granular, Process-by-Process Basis
This relates to how companies handle the requests that they've received. Currently, most companies that provide data on outcomes do so in aggregate. Only a few companies do so on a process-by-process basis (e.g., number of warrants responded to with content, number of warrants where account did not exist, etc.). We believe there is value in the more granular approach and we encourage all other companies to consider providing outcome-related data for each kind of legal process separately. Reporting outcomes on a granular, process-by-process basis can be a helpful tool for diagnosing problems or anomalies with respect to particular types of orders (e.g., pen registers being wrongfully used to obtain content of communications, or data that suggests a particular type of process is being used in a non-particularized way in order to obtain bulk user information).

Descriptive Outcome Reporting
Based on current practices, we recommend the following approach for describing the outcomes of requests. This approach has two overarching categories: requests rejected and requests not rejected, with three sub-categories for requests not rejected.

Requests Rejected: This is the number of requests denied in full. We recommend that companies offer a non-exclusive list of reasons for rejection, including invalid form or administrative mistake (e.g., misspellings, missing signatures, wrong company), invalid process for information requested, wrong jurisdiction, and improper process.[1]

Request Not Rejected: This is itself separated out into three sub-categories:

- No data disclosed. The company attempted to comply with the request but could not provide data, either because the account did not exist or the data sought was not in the account.
- Content disclosed. This may include non-content in addition to the content.
- Only non-content disclosed.

[1] *Yahoo's report, for example, states: "Yahoo may have possessed data responsive to the Government Data Request, but none was produced because of a defect or other problem with the Government Data Request (e.g., the government agency sought information outside its jurisdiction or the request only sought data that could not be lawfully obtained with the legal process provided). This category also includes Government Data Requests that were withdrawn after being received by Yahoo."*

There are a few additional opportunities for companies to adopt innovative approaches. For instance, separating "responded in part" from "responded in full" might help users understand where and when companies have worked to narrow government requests. Additionally, separating "no account exists" from "data sought does not exist within an account" might be useful because the absence of an account is perhaps a lesser privacy violation (because there was no account for the company/government to look into). In contrast, "data sought does not exist within an account" counts the number of times that governments successfully identified accounts and would have collected data but for the fact that the particular type of data requested did not exist.

As described above, we recommend that companies treat amended requests as new requests. When a company rejects a request for any reason (e.g., overbroad, incomplete, incorrect form) that would count as a rejection, even if the result is a new corrected or narrowed request. The subsequent amended request would be treated as a entirely new request.

OUTCOMES / COMPLIANCE WITH REQUESTS

SEARCH WARRANTS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

WIRETAP ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

PEN REGISTER ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

OUTCOMES / COMPLIANCE WITH REQUESTS (Cont'd)

OTHER COURT ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

CRIMINAL SUBPOENAS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

GOVT. CIVIL SUBPOENAS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

EMERGENCY REQUESTS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

TOTAL—ALL ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

User Notification

Several companies include in their reports information about when they have given notice to targets of government requests prior to disclosure of that information. Currently there are a wide variety of approaches taken to disclosing user notice. We recommend that companies follow a blend of several existing approaches and that they provide user notice both as a number and as a percent of the total number of requests. The information provided should cover:

- Requests accompanied by non-disclosure orders
- Requests without non-disclosure orders, for which notice was provided
- Requests without non-disclosure orders, for which notice was not provided

Depending on the company's definition, requests that are not responded to at all may be classified as providing no notice (which is Twitter's approach).

USER NOTIFICATION (PRE-DISCLOSURE)

	Requests with Non-Disclosure Orders	No Non-Disclosure Order, Notice <u>was</u> Provided	No Non-Disclosure Order, Notice <u>was not</u> Provided	TOTAL
# Received				
% of Total				100%

For companies able to and interested in providing additional information about user notification and non-disclosure orders, there are a few supplementary categories that might be considered:

- Average length of the non-disclosure order (a.k.a. average length of the seal) received during this time period
- Number of non-disclosure orders that are time-limited vs. the number of non-disclosure orders that are indefinite received during this time period
- Number of users notified after a non-disclosure order expired in this time period
- Number of notifications for newly unsealed orders in this time period

NATIONAL SECURITY ORDERS

PICKING A REPORTING STRUCTURE FOR NATIONAL SECURITY ORDERS

National security-related demands for user information, such as National Security Letters (NSLs) and court orders under the Foreign Intelligence Surveillance Act (FISA), are accompanied by a legal obligation not to disclose their existence. However, the USA FREEDOM Act of 2015 authorizes four different options for companies to publish numerical information about the NSLs and FISA orders they receive.[1]

None of the four different approaches allow reporting of specific numbers; instead they allow only banded ranges of numbers. Speaking generally, the smaller an option's band range is, the less granular the report is allowed to be with regard to the type of requests being made; the larger the band, the more specific companies can be about the different types of requests they've received. Similarly, the smaller the band, the more likely it is that the statute requires a longer delay before reporting, and/or a longer reporting period. As with all of our recommendations, we encourage you to discuss reporting on national security orders with your attorney.

Briefly summarized, the four options allow:

1. **Reporting in bands of 1000**, semiannually, covering a period of ≥ 180 days, with a 180-day delay for FISA process. There is no delay for NSLs, but reporting is limited to NSLs from the previous 180 days. This option allows for the most granularity in terms of types of process received, providing for separate reporting of the number of requests and the number of customer selectors targeted by NSLs, FISA orders for content, and FISA orders for non-content. Additionally, companies can report the specific number of customer selectors targeted for three different types of FISA non-content requests: pen register and trap and trace orders, orders for the ongoing production of call detail records, and orders for other business records. However, any reporting about FISA requests related to platforms, products or services that have not previously received FISA process must be delayed for 540 days (though this does not apply to new enhancements or iterations of existing platforms, products or services that already exist).
2. **Reporting in bands of 500**. This option is identical to Option 1, except that it does not allow the additional reporting on customers selectors targeted for the three different types of FISA non-content requests allowed under Option 1.
3. **Reporting in bands of 250**, semiannually, covering a period of ≥ 180 days, but with no delay. Here, however, companies are no longer able to break out numbers as between NSLs, FISA for content and FISA for non-content, but can only report a single number reflecting the total number of national security-related requests, and the total of customer selectors targeted by those requests.

[1] *See 50 U.S.C. 1874 for specific statutory language.*

4. **Reporting in bands of 100**, annually, covering a period of one year and delayed for at least one year. As with Option 3, only the total number of requests and the total number of targeted customer selectors can be reported.

Importantly, there is some lack of clarity regarding what exactly is counted as a "targeted customer selector" under this law. Under the 2014 Justice Department settlement regarding reporting on national security orders that preceded the USA FREEDOM Act, one of the reporting options allowed for reporting on the number of "customer selectors targeted" by FISA orders but only on the number of "customer accounts affected" by NSLs, indicating that they mean different things—presumably the number of customer identifiers specified in an order and the number of customer accounts that corresponded to those identifiers, respectively. So, the plain language of USA FREEDOM seems to only authorize the former number—but legislative history seems to indicate that it actually authorizes both or either of them. In a May 2015 report to the Committee on the Judiciary, Chairman Bob Goodlatte, bill sponsor, explained that the USA FREEDOM Act's "customer selectors targeted" language was "intended to capture circumstances in which the government asks the company for information about a single identifier or selector, but the company returns multiple accounts associated with that identifier or selector, or the reverse situation where multiple identifiers or selectors are tied to a single account—what we would think of as customer accounts affected. Therefore, we think that in addition to reporting on the number of **customer selectors targeted in a request**, companies may also or instead be permitted to report on the **number of accounts responsive to that request**. We recommend you discuss this approach with your attorney.

RECOMMENDED APPROACH

Looking at the chart that follows on the next page, a few trends become clear:

- Option 1 (bands of 1,000): Only a few companies—primarily telecommunications companies (like Comcast and Sprint), which typically receive the most requests—are using Option 1, which has the largest bands and the most granular reporting by type of process. However and importantly, they are not reporting the separate FISA numbers that the option allows, which means they are not taking full advantage of the option and the only benefit they derive from choosing it is the lack of any delay on NSLs. This is particularly unfortunate with regard to the telecoms, since one of the main reasons Congress allowed for the more specific reporting about FISA numbers was to help ensure that the new authority for ongoing demands for Call Detail Records was not abused to collect information in bulk. **We recommend that large telecommunications companies use Option 1** to the full extent the law allows.
- Option 2 (bands of 500): Most of the larger internet and software companies (e.g., Facebook, Google, and Microsoft), as well as a few telecommunications providers, use this option. These larger companies receive high volumes of requests but also want to be able to break out NSLs and FISA requests. **We recommend that very large internet companies, small to mid-size telecommunications companies, or companies that receive especially large numbers of requests use Option 2.**
- Option 3 (bands of 250): Smaller internet companies (LinkedIn, Dropbox) or large companies that historically receive fewer requests than their peers choose this option so they can better reflect their lower numbers, choosing more precise numbers over more precise categories. A few telecoms also use this option, presumably to take advantage of the lack of any delay. **We recommend that small-**

to-midsize internet companies or large companies that receive relatively few requests use Option 3, although ultimately we would prefer to see everyone other than large telecommunications companies using Option 2 to better allow for combination and comparison of numbers.

- Option 4 (bands of 100): No one uses this option, therefore **we do not recommend that anyone use Option 4.**

SURVEY OF POST-*USA FREEDOM ACT* NATIONAL SECURITY REPORTING PRACTICES (JUNE 2016)

Option 1 *0-999 Band*	**Option 2** *0-499 Band*	**Option 3** *0-249 Band*	**Option 4** *0-99 Band*	**0 / No Requests**
4 companies *9.8%*	8 companies *19.5%*	11 Companies *26.8%*	0 companies *0%*	14 companies *34.1%*
Comcast CREDO Mobile Sprint Twilio	AOL AT&T Facebook Google Microsoft Snapchat Verizon Yahoo	Amazon Apple CloudFlare DigitalOcean Dropbox Evernote GitHub LinkedIn Pinterest T-Mobile Time Warner Cable		Adobe Ancestry.com Automattic Cisco Etsy Inflection Kickstarter Let's Encrypt Lookout Mapbox Nest Tumblr Uber Wikimedia

Companies that have not published an updated report since the USA FREEDOM Act passed (or shortly thereafter) have been omitted. Four companies (9.8%) surveyed—23andMe, Reddit, Slack, and Twitter—don't report on national security orders.

Reporting "0" for All Categories

Notably, the USA FREEDOM Act limitations on what companies can report regarding national security process only apply to companies subject to a nondisclosure order regarding FISA or NSL process, therefore companies that have received no such process—about a third of the companies we have surveyed—simply report that they have received zero national security requests, rather than choosing one of the four options, and this is what we recommend for such companies.

Reporting "0" for Specific Categories

The USA FREEDOM Act's provisions apply to companies that have received FISA or NSL nondisclosure orders only "with respect to" the FISA or NSL process they have actually received. Companies that, for example, have not received any NSLs but have received FISA process could arguably choose Options 1, 2, or 3 for the FISA orders and report zero for the NSL category. Similarly, a company that has received FISA pen register orders but has not received any requests for records could arguably choose Option 1 and report zero for pen registers while reporting in bands of 0-1000 for the other categories. We believe this is a fair reading of the law and recommend that companies consider this approach. However, no company has yet taken this approach, nor

should you without first consulting a lawyer.

Reporting on Unsealed National Security Orders
In some cases, whether through litigation or legislative change, companies have been able to publish specific national security requests that they have received (after redacting specific details of the investigation). In such a cases, we've seen at least one company update its numeric reporting to change the range of NSLs received in the relevant time period from 0-x to 1-x, to reflect the request that they were allowed to publish. We recommend this more accurate approach to reporting as a best practice but you should consult with a lawyer first.

Reporting on the Number of Customer Selectors Specified and the number of Customer Accounts Responsive
As discussed above, we think there is a good argument that the law allows reporting of both of these numbers, and therefore recommend that companies consider this approach. However, no company has yet taken this approach, nor should you without first consulting a lawyer.

Updating Old Reports
Since passage of the USA FREEDOM Act, several companies (such as Facebook and Google) have gone back and revised the national security reporting they did under their 2014 settlement with the DOJ to make that reporting consistent with the USA FREEDOM reporting option they have since chosen, and some have also gone back and added national security numbers for years prior to the DOJ settlement. We recommend that other companies work with their legal counsel to update past reporting where allowed, and to signal within their reports where information has been changed and updated.

REPORTING NSLS & FISA ORDERS UNDER THE USA FREEDOM ACT

ORDERS ARE REPORTED ...	OPTION 1	OPTION 2	OPTION 3	OPTION 4
In bands of:	1,000 *Starting with 0-999*	500 *Starting with 0-499*	250 *Starting with 0-249*	100 *Starting with 0-99*
No more frequently than:	Semiannually	Semiannually	Semiannually	Annually
For a time period covering:	180 days	180 days	180 days	1 Year
With a mandatory reporting delay of:	NSLs: N/A FISA Orders: ≥ 180 Days [1]		N/A	≥ 1 Year

WHAT CAN BE REPORTED	OPTION 1	OPTION 2	OPTION 3	OPTION 4
# of National Security Letters	✓	✓		
# of FISA Orders for Content	✓	✓	✓ Combined	✓ Combined
# of FISA Orders for Non-Content	✓	✓		
# of Customer Selectors Targeted by National Security Letters	✓	✓		
# of Customer Selectors Targeted by FISA Orders for Content	✓	✓	✓ Combined	✓ Combined
# of Customer Selectors Targeted by FISA Orders for Non-Content	✓ [2]	✓		

[1] *Delay of 540 days if the "platform, product, or service" has not previously received a FISA order.*

[2] *For FISA orders for non-content, the reported number of customer selectors targeted can be disaggregated by legal authority, i.e., can report each of the following in its own band of 1,000: requests under Title IV (orders for pen register and trap and trace surveillance), Title V § 501(b)(2)(B) (orders for production of business records, not counting orders for ongoing disclosure of call detail records), and Title V § 501(b)(2)(C) (orders for ongoing production of call detail records).*

NATIONAL SECURITY REQUESTS

OPTION #1 *Bands of 1000 (semiannually)*	Nat'l Security Letters	FISA Orders for Content	FISA Orders for Non-Content		
# Received					
# of Customer Selectors Targeted			*Title IV* [1]	*Title V § 501(b)(2)(B)* [2]	*Title V § 501(b)(2)(C)* [3]
# of Accounts Responsive					

OPTION #2 *Bands of 500 (semiannually)*	Nat'l Security Letters	FISA Orders for Content	FISA Orders for Non-Content
# Received			
# of Customer Selectors Targeted			
# of Accounts Responsive			

OPTION #3 *Bands of 250 (semiannually)*	National Security Letters + FISA Orders for Content + FISA Orders for Non-Content
# Received	
# of Customer Selectors Targeted	
# of Accounts Responsive	

OPTION #4 *Bands of 100 (annually)*	National Security Letters + FISA Orders for Content + FISA Orders for Non-Content
# Received	
# of Customer Selectors Targeted	
# of Accounts Responsive	

[1] *Orders for pen register and trap and trace surveillance.*
[2] *Orders for production of business records, not counting orders for ongoing disclosure of call detail records.*
[3] *Orders for production of call detail records.*

REQUESTS FROM FOREIGN GOVERNMENTS AND LAW ENFORCEMENT ENTITIES

OUTSIDE THE U.S.: PROSPECTIVE & RETROSPECTIVE REQUESTS

RECOMMENDED APPROACH

Identifying ways to report international requests so that they are roughly comparable to U.S. legal processes is extraordinarily difficult for legal scholars, let alone compliance or policy personnel at a startup. In order to address this issue we recommend that companies take two steps:

1. Companies should classify requests by whether they are retrospective (for existing, historical user data) or prospective (for data that will be collected in the future).
2. Most importantly, companies should provide a narrative about international requests that helps put these requests into context. This narrative can highlight the variation in local laws, explain practices and standards in dealing with international requests, and any useful context. The narrative does not need to cover every single request, but it should draw attention to any significant events or requests.

Although no company is currently using this reporting method in their transparency reports, we recommend this approach for two reasons:

1. The prospective vs. retrospective distinction should be easy to make for employees without any legal or specialized knowledge.
2. It will allow for comparison between U.S. retrospective orders (warrants, subpoenas, etc.) and international retrospective orders, and between U.S. prospective orders (wiretaps and pen registers) and international prospective orders. We believe this will allow for the greatest global comparison.

This information should be reported on a country-by-country basis. However, depending on the number of countries in which a company operates and how many requests are received, aggregate reporting may make more sense.

TYPES OF LEGAL PROCESSES RECEIVED

	Retrospective [1]	Prospective [2]	TOTAL
# Received [3]			

[1] For existing, historical user data.
[2] For data that will be collected in the future.
[3] Total number of orders of any kind acted on (e.g., rejected or responded to) during [TIME PERIOD].

SELECTORS & ACCOUNTS FOR ALL OF THE ABOVE REQUESTS

Total # of Selectors Specified by All of the Above Requests		Total # of Accounts Potentially Affected by All of the Above Requests	

Finally, companies should report aggregate outcome/compliance and user notification data for international requests. The template does not include a column for disclosing content; ECPA prohibits U.S. companies from disclosing user content at the request of foreign governments. If companies are disclosing content to foreign governments for some reason, they should note that in their reports. Note that this is reporting on notification of users who have been the subject of a request prior to disclosure of that information.

OUTCOMES / COMPLIANCE WITH REQUESTS

	Rejected	No Data	Non-Content Disclosed	TOTAL
# Received				
% of Total				100%

USER NOTIFICATION

	Requests with Non-Disclosure Orders	No Non-Disclosure Order, Notice was Provided	No Non-Disclosure Order, Notice was not Provided	TOTAL
# Received				
% of Total				100%

OTHER REPORTING PRACTICES TO CONSIDER

NON-COUNTING & QUALITATIVE FEATURES

Below are some additional recommendations and considerations for companies publishing transparency reports. These recommendations focus on the "qualitative" elements of the report as well as publishing logistics.

RECOMMENDED APPROACHES

Structured Data Format
We recommend that companies make all data available in a CSV (comma separated values) format. Many companies choose to publish their reports as PDFs which makes for easy downloading and carries company branding. Similarly, others chose to publish their reports as a website with embedded data tables, which can allow readers to easily flip between years and other subsets of the data. However, for researchers, journalists, and others who want to make use of the report data, these formats are less helpful because the data extraction processes can be tedious and time-consuming. Publishing all data as a CSV file in addition to the full report will make transparency reporting more accessible.

Permanent Location for Reports
We recommend that all reports—both current and archived—have easily accessible permanent homes/links. Reports can be linked to from corporate blog posts, PDFs, and/or transient links, but those should not be the only way to access the report. Some companies create a dedicated permanent URL with embedded data and other report content (FAQs, glossary, narrative or introductory information). Other companies have a dedicated webpage that provides links to downloadable data files (PDFs and/or CSVs), rather than embedded text and data. Regardless of the webpage's setup, the page should include static links to information that will help readers better understand your report, such as relevant policies (e.g., for notifying users), FAQs, a glossary, and explanations of how requests for user information are processed.

Licensing
We recommend that all companies use a non-restrictive Creative Commons license for their reports, such as the "ShareAlike" license, which "lets others remix, tweak, and build upon your work even for commercial purposes, as long as they credit you and license their new creations under the identical terms." For more information on Creative Commons licensing, visit https://creativecommons.org/licenses/, and for information about choosing a Creative Commons license, visit https://creativecommons.org/choose/.

Narrative for the Report
We suggest that companies take the opportunity of producing a transparency report to develop a narrative statement that turns their report into a story about company values, policies, and user trust. Transparency reporting is a tremendous opportunity for companies to tell their story, and the narrative is the place to do that, as well as to provide context to the report as a whole. In particular, the narrative can

be used to highlight, explain, and elaborate upon:

- The services that are included in the report, the services that are not included, and why
- Information about notable events that may have influenced the numbers in the report, such as the release of a new product or service, a change in company collection policies, and political event that changed government behavior
- Explanations for numbers that changed significantly between one report to the next
- How the company's business model and services affect government requests, such as company practices to not collect certain kinds of information
- A narrative need not be very complex or long (our template includes modifiable boilerplate narrative) but it should highlight some of the key elements that companies hope readers take away from the report.

Glossary / Definitions for the Report

Defining legal processes and other key terms that appear in a transparency report is an often overlooked—but key—part of the report. While many readers of reports may be attorneys, civil society members, policy personnel, or others well-versed in legal terminology, there are many readers who are unfamiliar with the legal processes or sources of law that appear in these reports. Companies should aim to increase the accessibility of their reports, and one relatively easy way to do that is by making the report's text simple for non-lawyers, and including a glossary. A glossary explaining legal processes and other key terms used in the report can both inform readers about the types of processes that might allow governments to access their data, while also helping everyone understand some of the logistics behind transparency reporting, such as how companies are counting legal processes (particularly in more nebulous categories like court orders). For those companies that do not have the resources to independently create a glossary, we have included definitions in our template as a starting point. The definitions we've included draw upon those identified as best practices in *Transparency Reporting Toolkit* Memo 2: Defining Legal Processes.

FAQ: Frequently Asked Questions for the Report

For companies with the capacity to include additional information in their reports, a "frequently asked questions" section is a helpful addition. While a lot of important information will already be covered elsewhere in the report (such as the companies' values and an explanation of why the company publishes a transparency report in the narrative, and definitions of key terms in the glossary), a FAQ goes above and beyond to inform readers about company practices and how legal process requests are handled. This section could explore a number of topics from the company side (e.g., how requests work their way through the company's internal departments or external legal counsel, what information or requests might be exempted or excluded from the report, how the company has worked to narrow requests for information) as well as the government/law enforcement side (e.g., how a law enforcement agency goes about obtaining a search warrant or an emergency disclosure, how a company handles requests from outside of the United States). For one unique and engaging approach to explaining these topics, check out Google's "Way of a Warrant" video, which walks viewers through the company's processes for reviewing and responding to ECPA search warrants.

UNCOMMON BEST PRACTICES & OTHER NOTABLE IDEAS

UNCOMMON BEST PRACTICES

We have tried to base our recommendations on things that are consensus best practices among existing transparency reports, and have noted where our recommendations diverge from current consensus behaviors. However, we have identified a few areas where companies may consider adopting practices that are not yet widespread, but could be beneficial, such as including the following data points:

- Breaking out requests by agency
- Breaking out requests by government level (e.g., federal vs. state vs. local)
- State-by-state numbers
- Specific information on location requests
- Breaking out data by product or service
- Total number of users (or some other indication of the scope of requests compared to scope of the user base)

Companies might consider submitting redacted versions of all government requests to Lumen Database (https://lumendatabase.org, formerly Chilling Effects) in order to create a catalog of reports that can be used to improve these recommendations and help people better understand government requests.

TRANSPARENCY REPORTING TEMPLATE

[COMPANY NAME / LOGO]

TRANSPARENCY REPORT ON GOVERNMENT AND LAW ENFORCEMENT REQUESTS FOR USER INFORMATION

Covering the Period of: Month, Year—Month, Year

Date Published: MM/DD/YYYY

.

Report © [YEAR] [COMPANY] under CC BY SA

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.
To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-sa/4.0/.

FRONT MATTER: INTRODUCTION TO THE TRANSPARENCY REPORT

INTRODUCTION

[Company Name] is pleased to release our [first/second/third/...] transparency report covering the [first half/second half] of [year].

ABOUT OUR TRANSPARENCY REPORT

Like many other [technology/telecommunications/social media/...] companies, we sometimes receive requests from law enforcement agencies in both the United States and abroad who seek information about our users relating to criminal [and civil/intelligence/law enforcement...] investigations. We have a legal obligation to respond to valid government requests for user data. Similarly, we believe that we have a duty to inform our users and the public at large about those requests, and that is why we have prepared this transparency report.

Many companies release transparency reports because they care about the privacy and security of their users and want to demonstrate that commitment. This section provides an opportunity for a company to highlight the important elements of their corporate philosophy.

Protecting our users' privacy is very important to us. For that reason, we carefully review each request for user data, and work with law enforcement to narrow such requests where possible. Our aim is to fully meet our legal obligations while honoring the trust that our users place in us and our services.

If a company's transparency report covers other areas in addition to requests for user data, the company should indicate that here.

This transparency report provides information relating to law enforcement requests for user data [and government requests for content removal/intellectual property takedown notices/terms of service enforcement/...] that we processed between [Month day, year] and [Month day, year].

REPORT SUMMARY

This space provides an opportunity for the company to point out any significant trends in their data, and to place those trends into a larger context that helps explain the changes.

During this period we received a total of [number] requests for user information from U.S. law enforcement agencies. This is a[n] [increase/decrease] from the [number] requests we processed in the previous period covering [Month day, year] to [Month day, year]. This [increase/decrease] is in part attributable to [description of any notable events, such as

If there are any changes in the transparency report data that are surprising or unusual, this would be a good place to highlight those and explain why the data may have changed.

Some companies have a business model or corporate practices that affect the kinds of data they collect, retain, and are able to provide to law enforcement or intelligence agencies. This space is an opportunity for a company to describe those practices and how those practices impact their transparency report.

Not every company will need to address MLATs or the All Writs Act, but those that do should consider addressing them in these specific sections that help explain their significance to readers.

change in users, entering a new market, the introduction of new product, a change in transparency reporting approach, a political event, etc.].

We specifically want to call attention to [specific number or section that changed significantly since the last report]. In our [date of previous report] transparency report, we received [X number of processes], and in this period there were [Y number of processes]. One reason for this change is [description of any notable events, such as change in users, entering a new market, the introduction of new product, a change in transparency reporting approach, a political event, etc.].

In this reporting period we received [number of requests] for [particular kind of content]. However, we are unable to provide that [particular kind of content] to law enforcement because we do not track that data for our customers.

ADDITIONAL FEATURES

MLAT Requests

A Mutual Legal Assistance Treaty (MLAT) is a treaty between the U.S. and another country that establishes a process for the two country to assist each other in criminal investigations. The MLAT process provides a way for foreign governments to ask the U.S. government to issue a request for user information. Requests that comes through the MLAT process sometimes say so, but often they appear to be identical to any domestic request for information. In this reporting period [X percent] of the search warrants and [Y percent] of court orders we received were explicitly identified as having been issued through MLAT procedures. These requests came from [#] different countries, including [list of countries].

All Writs Act

The All Writs Act is a federal law from 1789 under which courts can authorize orders ("writs") that compel a party to take a particular action. Following the December 2015

The primary recommendation of this guide is that companies should be clear about what they are counting and how they are counting in their transparency report. Following the recommendations of this guide can help explain those practices, but companies should be clear when their practices diverge from the recommended practices.

Companies should be clear about which of their services are included in this report, and direct readers to other relevant transparency reports.

It is important for companies to describe any practices that significantly impact the data in the report, or that help readers understand how the data in the report is calculated.

San Bernardino shooting, the U.S. government attempted to use the All Writs Act to compel Apple to circumvent the encryption of an iPhone seized during the investigation, resulting in increased public interest in requests made under this law. During the period of [current reporting period] we [have/have not] received any orders under the All Writs Act of 1789 asking us to [redesign our service / facilitate search or surveillance / etc.].

HOW TO READ THIS REPORT

General Approach
Throughout this report we generally adopt the definitions and best practices described in the *Transparency Reporting Toolkit's Reporting Guide and Template* created by the Open Technology Institute at New America and the Berkman Klein Center for Internet & Society at Harvard University. We make every effort to note where our definitions or approach is different than those in the Toolkit.

Services Covered
[Company name] offers many different products and services, including [list of various products]. This transparency report covers [all/some] of these products and services. This transparency report does not cover government requests regarding [not included service name]; information about those requests are available on the [not included service name] transparency report, available here <link>.

Important Company Practices
In responding to requests we make several important determinations to ensure that we fully complying with lawful requests while respecting the privacy of our users. These decisions include:

- Reasons for rejecting requests: We review all government requests carefully. There are many reasons why we may conclude that a request is deficient and should be rejected. These may include: [list of reasons why

company might reject a request].

- Counting Selectors: At several points in this report we talk about the number of "selectors" in a request. A selector simply an identifier [e.g. a username, IP address, e-mail address, phone number, etc.] specified by law enforcement in legal process when requesting user information. When counting the number of selectors, we [description of how the company counts selectors.

INTERNATIONAL REQUESTS

Although [company name] is a U.S. company, we have a corporate presence in several other countries. Because of that, we respond to requests in all countries that have legal jurisdiction over our operations. When we receive requests from non-US governments we [description of practices for handling such requests, including working with local counsel, referring to documents of guiding principles, etc.].

In this reporting period we saw a significant [increase/decrease] in requests from [specific country]. This appears to be a result of [significant local event in that country, such as passing a new law, etc.]. [Note any other significant data points from international requests and place it into the appropriate context].

Changes in international requests often reflect changing political and economic circumstances. The narrative is a good place for a company to provide helpful context and identify any significant events that have impacted the international requests they received.

ACKNOWLEDGMENTS

This transparency report is based on the *Transparency Reporting Toolkit's Reporting Guide and Template* created by the Open Technology Institute at New America and the Berkman Klein Center for Internet & Society at Harvard University. For more information about transparency reporting and the process of creating a transparency report, you can read the entire Toolkit at: https://www.newamerica.org/oti/transparency-toolkit/.

UNITED STATES REQUESTS

TYPES OF LEGAL PROCESSES RECEIVED

	Search Warrants	Wiretap Orders	Pen Register / Trap and Trace Orders	Other Court Orders	Subpoenas		Emergency Requests	TOTAL
					Criminal	*Civil*		
# Received [1]								

SELECTORS & ACCOUNTS FOR ALL OF THE ABOVE REQUESTS

Total # of Selectors Specified by All of the Above Requests		Total # of Accounts Potentially Affected by All of the Above Requests	

PRESERVATION REQUESTS

# Received	# of Selectors Specified	# of Accounts Responsive

USER NOTIFICATION (PRE-DISCLOSURE)

	Requests with Non-Disclosure Orders	No Non-Disclosure Order, Notice <u>was</u> Provided	No Non-Disclosure Order, Notice <u>was not</u> Provided	TOTAL
# Received				
% of Total				100%

[1] *Total number of orders of any kind acted on [e.g., rejected or responded to] during [TIME PERIOD].*

OUTCOMES / COMPLIANCE WITH REQUESTS

SEARCH WARRANTS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

WIRETAP ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

PEN REGISTER ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

OTHER COURT ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

UNITED STATES REQUESTS (CONT'D)

OUTCOMES / COMPLIANCE WITH REQUESTS (Cont'd)

CRIMINAL SUBPOENAS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

GOVT. CIVIL SUBPOENAS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

EMERGENCY REQUESTS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

TOTAL—ALL ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests					
% of Total					100%

NATIONAL SECURITY REQUESTS

OPTION #1 *Bands of 1000 (semiannually)*	Nat'l Security Letters	FISA Orders for Content	FISA Orders for Non-Content		
# Received					
# of Customer Selectors Targeted			*Title IV* [1]	*Title V § 501(b)(2)(B)* [2]	*Title V § 501(b)(2)(C)* [3]
# of Accounts Responsive					

OPTION #2 *Bands of 500 (semiannually)*	Nat'l Security Letters	FISA Orders for Content	FISA Orders for Non-Content
# Received			
# of Customer Selectors Targeted			
# of Accounts Responsive			

OPTION #3 *Bands of 250 (semiannually)*	National Security Letters + FISA Orders for Content + FISA Orders for Non-Content
# Received	
# of Customer Selectors Targeted	
# of Accounts Responsive	

OPTION #4 *Bands of 100 (annually)*	National Security Letters + FISA Orders for Content + FISA Orders for Non-Content
# Received	
# of Customer Selectors Targeted	
# of Accounts Responsive	

[1] *Orders for pen register and trap and trace surveillance.*

[2] *Orders for production of business records, not counting orders for ongoing disclosure of call detail records.*

[3] *Orders for production of call detail records.*

INTERNATIONAL REQUESTS

TYPES OF LEGAL PROCESSES RECEIVED

	Retrospective [1]	Prospective [2]	TOTAL
# Received [3]			

SELECTORS & ACCOUNTS FOR ALL OF THE ABOVE REQUESTS

Total # of Selectors Specified by All of the Above Requests		Total # of Accounts Potentially Affected by All of the Above Requests	

USER NOTIFICATION

	Requests with Non-Disclosure Orders	No Non-Disclosure Order, Notice was Provided	No Non-Disclosure Order, Notice was not Provided	TOTAL
# Received				
% of Total				100%

[1] *For existing, historical user data.*

[2] *For data that will be collected in the future.*

[3] *Total number of orders of any kind acted on (e.g., rejected or responded to) during [TIME PERIOD].*

INTERNATIONAL REQUESTS (CONT'D)

OUTCOMES / COMPLIANCE WITH REQUESTS

	Rejected	No Data	Content Disclosed	Non-Content Disclosed	TOTAL
# Received					
% of Total					100%

GLOSSARY / DEFINITIONS

These definitions are an amalgamation of existing transparency report glossaries and encompass the best practices in defining legal processes as identified in *Transparency Reporting Toolkit Memo 2: Defining Legal Processes*.

U.S. LEGAL PROCESSES TERMS

2703(d) Court Orders
Often known as a "d order" or ECPA order, § 2703(d) court orders are granted based on an intermediate standard that is less stringent than the probable cause standard for warrants, but more demanding than the mere relevance standard required for subpoenas. To receive an ECPA court order, a law enforcement agency must present specific and articulable facts to a judge or magistrate demonstrating that there are reasonable grounds to believe the requested information is relevant and material to an ongoing criminal investigation. The orders compel an internet service provider to disclose more information than is usually obtainable by subpoena, like records relating to a subscriber other than the contents of communications. This could include the IP address associated with a particular email sent from that account or used to change the account password (with dates and times) and the non-content portion of email headers such as the "from," "to" and "date" fields. An ECPA court order is available only for criminal investigations.

Other Court Orders
Other court orders refers to valid and binding orders issued by local, state, or federal courts, other than the court orders counted separately (e.g., search warrants, pen register and trap and trace orders, etc.). Such orders generally seek historical information and more detailed information than is available using a subpoena. To obtain a court order, a judge must sign the order indicating that the law enforcement entity seeking the court order has made the requisite showing under the law to obtain the order.

Emergency Request/Disclosure
Also referred to as exigent requests or emergency disclosures, these are voluntary disclosures made to a government agency seeking information to save the life of a person who is in peril or prevent serious physical injury. These disclosures are made when the company has reason to believe that doing so is necessary to prevent death or serious physical harm to someone. Emergency requests must contain a description of the emergency and an explanation of how the information requested might prevent the harm. The information provided in response to an emergency request is limited to what the company believes would help prevent the harm. Examples of situations where emergency requests might be necessary would include

kidnappings, missing person cases, attempted suicides, etc.

Search Warrant
Also known as probable cause court orders or warrants, a search warrant is a court order granted based on a showing of probable cause, the highest standard to obtain evidence. To successfully receive a warrant, government agencies are required to provide evidence of "reasonable ground to suspect that a person has committed or is committing a crime, or that a place contains specific items connected with a crime." The order must be supported by sworn testimony and sufficient evidence, and must specifically identify the place to be searched and the items to be seized. Except in emergency circumstances, a search warrant is required before the company will disclose stored content (e.g., documents, photos, e-mails and voice messages).

Subpoena
A subpoena is a legal demand issued directly by a prosecutor or a law enforcement or administrative agency to a company, usually without prior court approval. A prosecutor or agency can issue a subpoena when they determine that the material sought is relevant to a civil or criminal investigation. Of all of the types of legal process, subpoenas require the lowest standard of proof. However, subpoena can only be used to compel disclosure of non-content information—for example, basic subscriber information, name and address, IP address, call records, or sign-in and sign-out records.

Pen Register/Trap and Trace Order (PRTT)
PRTT orders are court-issued orders used to authorize the real-time, prospective collection of non-content dialing or addressing information (sometimes called "metadata") about the incoming and outgoing communications of a target in real time. Such information may include phone numbers, email addresses, IM handles, IP addresses, and the domain name of web sites visited (i.e., everything before the / in the web address), as well as time stamps and the size or length of the communication. Trap and trace orders apply to information about incoming communications while pen registers apply to information about outgoing communications, and the two orders are usually issued in combination. It's easier for a government agency to get a PRTT order than wiretap order or search warrant. Rather than presenting facts that demonstrate probable cause, they need only certify that information likely to be obtained will be relevant to an ongoing criminal investigation. PRTTs typically last 60 days, and can be renewed for additional 60 day periods. Unlike with wiretaps, there is no requirement that the user be notified after the surveillance is completed.

Wiretap Order

A wiretap order is judge-issued order that requires a wire or electronic communications provider to provide to law enforcement real-time access to the content of communications. The order can relate to the content of telephone or internet communications. When compared to other kinds of legal process, wiretap orders are the most difficult for law enforcement to obtain. In order to obtain a wiretap order, a government agency must demonstrate probable cause that: a) someone is committing one of certain offenses specified in the Wiretap Act, b) the wiretap will collect information about that crime, and c) the crime involves the telephone number or account that will be tapped. Before issuing the wiretap order, the court must also find that other, less intrusive investigatory techniques have failed (or probably would fail), or are too dangerous to attempt. Wiretap orders run for 30 days (which can be renewed) and the court must generally notify the subjects of wiretap orders with a reasonable time after the conclusion of the wiretap.

NATIONAL SECURITY TERMS

Foreign Intelligence Surveillance Court (FISC) Order

Also knows as FISA requests or FISA orders, Foreign Intelligence Surveillance Court orders are secret demands that can require U.S. companies to hand over or assist in the monitoring of users' communications content and non-content data. The Foreign Intelligence Surveillance Act (FISA) is a U.S. law, originally enacted in 1978, to govern how the U.S. government collects foreign intelligence for national security. As with the regular court system in regular criminal investigations, the FISA-created Foreign Intelligence Surveillance Court can issue wiretap (or "electronic surveillance") orders, search warrants, PRTT orders, and orders for non-content records ("Section 215 orders"). However, unlike in the regular court system, FISC orders do not require probable cause of a crime, and all FISC orders are accompanied by an indefinite gag order (although companies are now allowed under the USA FREEDOM Act of 2015 to report aggregate data about the FISC orders they receive). In addition to providing for individualized surveillance demands as in criminal cases, FISA—as amended by the FISA Amendments Act of 2008—also allows for the issuance of non-individualized surveillance orders authorizing broad programs of surveillance that can target any person outside of the U.S., including their communications with people inside the U.S., so long as those communications are believed to have foreign intelligence value. In these cases, the court does not approve specific targets, but instead approves the government's own guidelines for how it picks its targets and minimizes non-pertinent data.

National Security Letter

Also known as national security demands or national security requests, national security letters (NSL) are secret subpoenas issued by the Federal Bureau of Investigations under 18 U.S.C. §

2709, a part of the Electronic Communications Privacy Act (ECPA). In order to obtain an NSL, the Director of the FBI or a senior FBI designee or the special agent in charge of a local FBI field office must provide a written certification that demonstrates the information requested is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. NSLs can only be used to obtain non-content, like certain basic subscriber and transactional information. Companies can only disclose the receipt of NSLs in aggregate amounts, as described in the USA Freedom Act.

NON-U.S. LEGAL PROCESS TERMS

Prospective Order
An order for the real-time collection of information that will be generated in the future, such as the content and metadata associated with phone calls and e-mails that the target will send during the period in which the order is active.

Retrospective Order
An order for the collection of information that a company already has about and from the target, such as the content and metadata associated with phone calls and e-mails that the target sent using the systems owned by the company receiving the order.

SOURCES OF LAW

Electronic Communications Privacy Act (ECPA)
The Electronic Communications Privacy Act is a United States federal statute that prohibits a third party from intercepting or disclosing communications without authorization. The Act, which was originally passed as an amendment to the Wiretap Act of 1968, applies to both government employees and private citizens. It protects communications in storage as well as in transit.

The Act consists of three parts. The first, often referred to as "the Wiretap Act" or "Title III," outlaws the unauthorized interception of wire, oral, or electronic communications and establishes a judicial supervised procedure to permit such interceptions for law enforcement purposes. The second, the Stored Communications Act (SCA), focuses on the privacy of, and government access to, stored electronic communications. The third, typically referred to as "the Pen Register Statute," creates a procedure for governmental installation and use of pen registers as well as trap and trace devices. It also outlaws such installation or use except for law enforcement and foreign intelligence investigations.

GLOSSARY / DEFINITIONS (CONT'D)

Foreign Intelligence Surveillance Act (FISA)
The Foreign Intelligence Surveillance Act is a U.S. law, originally enacted in 1978 to govern how the U.S. government collects foreign intelligence for national security. This Act created the Foreign Intelligence Surveillance Court, which consists of 11 federal district court judges who review government applications for electronic surveillance and other types of intelligence collection. The FISA Amendments Act, passed in 2008, enables the court to require U.S. companies to provide information and the content of communications associated with the accounts of non-U.S. citizens or non-lawful permanent residents who are located outside the United States, as well as certain U.S. persons, subject to certain limitations. The DOJ oversees the agencies involved in carrying out FISA-authorized activities. FISA requires these agencies to brief Congress on a regular basis and present all pertinent FISA court documents.

Pen Register Statute
The federal criminal pen register statute was enacted in 1986 as part of ECPA to govern real-time interception of telephone numbers dialed or transmitted. The statute establishes the process for obtaining pen register and trap and trace orders. In 1998, Congress amended FISA to authorize the government to use pen registers to collect foreign intelligence information in national security investigations after obtaining an order from the Foreign Intelligence Surveillance Court.

Stored Communications Act (SCA)
The Stored Wire and Electronic Communications and Transactional Records Access, commonly referred to as the Stored Communications Act, was enacted in 1986 as part of the Electronic Communications Privacy Act. The Act addresses voluntary and compelled disclosure of stored communications held by third-party internet service providers.

The Act distinguishes between privacy protections for two types of network service providers: electronic communication service providers and commercial service providers. The statute creates two kinds of protections for customers. First, the Act enacts a broad prohibition against providers voluntarily sharing customers' communications with the government or others, subject to certain enumerated exceptions. Second, it outlines procedures permitting the government to require the disclosure of customers' communications or records. The statute applies to both content and non-content information.

Wiretap Act
Also known as Title III, the Wiretap Act was enacted in 1968 as part of the Omnibus Crime Control and Safe Streets Act of 1968. The Act provides protection against intentional and non-consensual interception of electronic communications, establishes procedures for the government to

obtain warrants to authorize wiretapping, and regulates the disclosure and use of authorized intercepted communications by investigative officers. The Act imposes a stringent warrant requirement before investigators can obtain a wiretap order.

OTHER TERMS USED

Accounts Responsive
This term describes the number of accounts that are responsive to a government request for information. These are the accounts that satisfy the elements of the government request after the company searches their records using the various selectors specified by law enforcement in the legal process (i.e. username, IP address, e-mail address, phone number, etc.). An individual may have multiple accounts, or a single account may be used by many people; the number of accounts responsive is only a rough proxy for the number of impacted individuals.

Selectors Specified
Also referred to as account identifiers or users/accounts specified, selectors specified refers to the number of identifiers (i.e. username, IP address, e-mail address, phone number, etc.) specified by law enforcement in legal process when requesting user information. Some legal processes may include more than one identifier, and multiple identifiers may be used to try to identify a single account.

Process Received
Process received describes the individual requests for information that an internet or telecommunications company has received. In transparency reports, companies disclose the specific number of each type of legal process received. These include search warrants, subpoenas, 2703(d) orders, emergency requests, wiretap orders, and pen register orders.

Non-Disclosure Order
A company may be prohibited from notifying users about a legal request for their information for some period of time. These prohibitions may take the form of a statute, court order, or some other limitation that prevents the company from providing notice to the user prior to complying with the request for information.

Content
Content refers to the information concerning the substance, purport, or meaning of a particular communication, which can include the text of e-mails, text messages, direct messages, Tweets, videos, and more. Obtaining content generally requires law enforcement to secure a warrant.

GLOSSARY / DEFINITIONS (CONTINUED)

What is considered content can be platform and service dependent and may be subject to disagreement between law enforcement and companies.

Non-Content
Non-content user information includes any and all account information that is not considered to be content. This can include basic subscriber information such as the name used to create an account, the IP address from which an account was created, or the IP address used to sign in to an account, along with dates and times. Non-content information can also include more detailed transactional data about a user's communications such as the IP addresses, email addresses, IM handles, or phone numbers that sent or received the communications, as well as when the communications occurred, how long in duration, and how large in size they were. The legal standard that law enforcement must meet depends on the exact kind of information they seek to obtain (see section on U.S. Legal Process Terms).

Request Rejected
A request is considered to be rejected when a company denies a request in full, providing neither non-content nor content information about the specified account or accounts. Companies generally reject requests due to some defect in the request, such as invalid process, the request is served on the wrong company, the request fails to specify an account, or it was duplicative of a previous request. A request can also be considered rejected when law enforcement withdraws the request; a request is not considered rejected when a company cannot find the specified information while attempting to comply with the request.

Content Disclosed
When a company indicates that it has disclosed content in response a government request, that disclosure may also include non-content information.

Only Non-Content Disclosed
When a company indicates that it has disclosed only non-content in response to a government request, that means they have provided no content in response to the request. Anytime a company provides content information in response to a request, it should count that as "Content Disclosed" even if non-content information was also provided.

No Data Disclosed
A company can indicate that no data was disclosed when in response to a government request the company attempted to comply but could not provide data either because the account did not exist, or the data sought was not found in the account. This is different from when a request is rejected and the company did not attempt to comply with the request.

