

DIGITAL ACCESS TO SCHOLARSHIP AT HARVARD
DASH.HARVARD.EDU

HARVARD LIBRARY


# The Transparency Reporting Toolkit: Best Practices for Reporting on U.S. Government Requests for User Information

## Citation

Woolery, Liz, Ryan Budish, and Levin Bankston. 2016. "The Transparency Reporting Toolkit: Best Practices for Reporting on U.S. Government Requests for User Information." The Berkman Klein Center for Internet & Society.

## Published version

https://cyber.harvard.edu/publications/2016/transparency_memos

## Link

http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552578

## 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

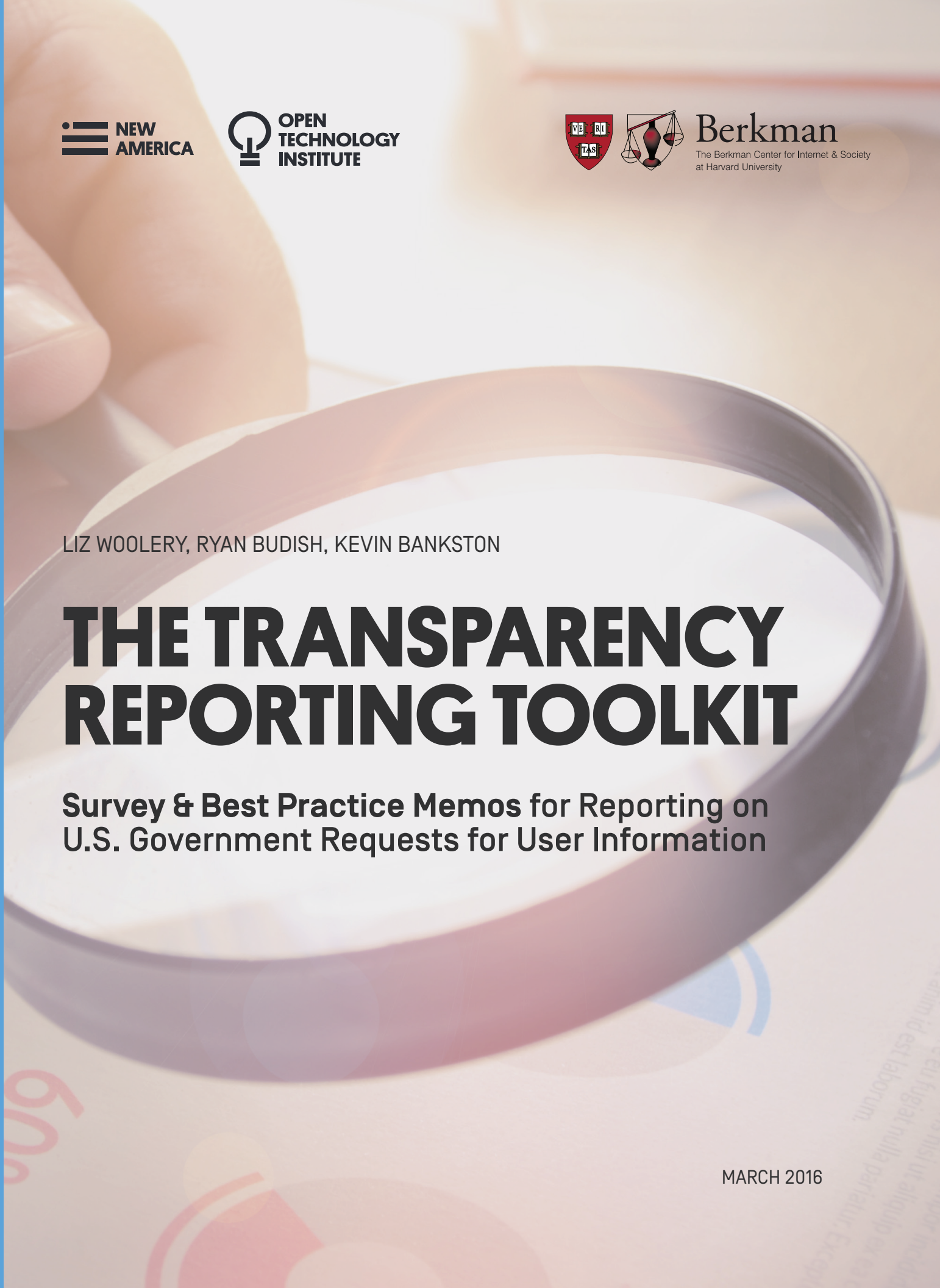
https://harvardwiki.atlassian.net/wiki/external/NGY5NDE4ZjgzNTc5NDQzMGIzZWZhMGFlOWI2M2EwYTg

## 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
The Berkman Center for Internet & Society at Harvard University

LIZ WOOLERY, RYAN BUDISH, KEVIN BANKSTON

# THE TRANSPARENCY REPORTING TOOLKIT

## **Survey & Best Practice Memos** for Reporting on U.S. Government Requests for User Information

MARCH 2016

**Report © 2016 NEW AMERICA and THE BERKMAN 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 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 Center for Internet & Society, rbudish@cyber.law.harvard.edu
Liz Woolery, 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 and members of the i2C Coalition, Rob Faris, Urs Gasser, Jess Hemerly, Robyn Greene, Priya Kumar, Colin Maclay, OTI Open Web Fellow Gemma Barrett, 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**

The Open Technology Institute at New America 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.

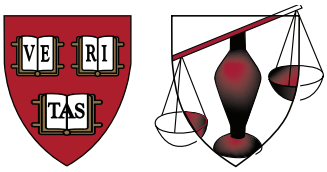
**ABOUT THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY**

Founded in 1997, the Berkman 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

The Berkman Center for Internet & Society
at Harvard University

**WITH GENEROUS SUPPORT FROM**

MacArthur Foundation

# TABLE OF CONTENTS

**PREFACE** ..... **1**

Introduction ..... 2

Quick Look: Overview of the Survey & Best Practice Memos ..... 4

Transparency Reports by U.S. Internet & Telecom Companies ..... 6

A Brief Introduction to U.S. Law on Government Access to Communications Data ..... 10

**SURVEY & BEST PRACTICE MEMOS** ..... **15**

Memo 1: Reporting on Different Legal Processes ..... 17

Memo 2: Explaining Legal Processes ..... 25

Memo 3: Reporting on the Subjects of Requests & How Users are Impacted ..... 39

Memo 4: Reporting on the Legal Processes Required for User Information ..... 51

Memo 5: Explaining "Content" & "Non-Content" ..... 61

Memo 6: Reporting on Outcomes & Compliance with Requests ..... 73

Memo 7: Reporting on User Notification ..... 93

Memo 8: Reporting on National Security Orders ..... 103

**INDEX** ..... **115**

# PREFACE

# INTRODUCTION

**ABOUT THE TRANSPARENCY REPORTING TOOLKIT**

The Transparency Reporting Toolkit is a project by New America's Open Technology Institute (OTI) and Harvard University's Berkman Center for Internet & Society. Using research on the current state of transparency reporting, the project aims to identify best practices, create a template transparency report, and establish reporting guidelines. These resources will be shared publicly to foster standardization in reporting and provide companies new to reporting with an easy-to-use set of tools essential to crafting their transparency reports.

Starting over two years ago, we began conducting interviews with companies about their processes for creating transparency reports in order to identify lessons that could be helpful to companies that had not yet created reports. Building off of that work, in November 2013, the Berkman Center for Internet & Society, in conjunction with the Center for Democracy & Technology, the Open Technology Institute, the Global Network Initiative, and others, convened a dialogue at the University of California, Berkeley with academics, civil society, and representatives from a variety of Internet companies. That meeting was followed by an East Coast convening, hosted by OTI in July 2014, with strong civil society and academic representation. Those dialogues informed these materials.

**What's in The Transparency Reporting Toolkit?**
In total, The Transparency Reporting Toolkit has three components, each of which informs the others:

1. **Survey & Best Practice Memos** (March 2016)
2. **Reporting Guide & Template** (Draft, March 2016
3. **Online Portal** (Spring/Summer 2016)

**ABOUT THE TOOLKIT'S SURVEY & BEST PRACTICE MEMOS**

Those conversations highlighted a variety of practices, open questions, and tensions within the area of transparency reporting, as well as the need for tools that could aid in the creation and standardization of reporting. One tool highlighted as a priority for development was a template that would help companies standardize their reporting while engaging in best practices. But those standards and best practices needed to be identified first. We set out to scope the landscape of transparency reporting and identify best practices, which led to the creation of this document. We began by surveying reports from 43 U.S. companies reporting on requests for user data from government and law enforcement agencies in the U.S. From there, we identified best practices in reporting. The result is a nearly comprehensive survey of the state of transparency reporting by Internet and telecommunications companies in the U.S. during the first half of 2015.

There are eight memos in the Transparency Reporting Toolkit, each surveying a different topic related to how U.S. Internet and telecommunications companies report on requests for user and customer information. These memos are limited to transparency reporting on data collection subject to U.S. federal

and state laws. Transparency reporting on data collection from other countries presents a separate opportunity to examine current and best practices. However, given the complexity of legal processes, compliance, and definitions on a global scale, we have limited the scope of this survey to U.S. companies subject to U.S. laws and requests for user information.

Each memo includes a survey of the current transparency reporting practices of 43 U.S. Internet and telecommunications companies. Each memo also highlights and explains the "best practices" in transparency reporting and identifies companies engaged in those practices.

**Scope of the Survey & Best Practice Memos**
What's covered in the Memos:

- Transparency reports issued by 43 U.S. Internet and telecommunications companies. A list of companies surveyed and links to their reports begins on page 6.
- All transparency reports surveyed were issued prior to July 10, 2015.
- The survey is limited to reporting on requests for information from U.S. government and law enforcement entities.

What's not covered in the Memos:

- Reports issued by foreign Internet and telecommunications companies.
- Reports issued after July 10, 2015.
- Reporting on requests from non-governmental entities.
- Reporting on requests from foreign governments and law enforcement entities.

**WHAT'S NEXT**

Having surveyed the landscape of transparency reporting and identified best practices in reporting, we are working to translate that research into a template and guide to best practices. The result will be The Transparency Reporting Toolkit's *Template & Guide to Reporting*, set to be released in Spring 2016. With the *Survey & Best Practice Memos* completed and the *Template & Guide to Reporting* in progress, the final piece of the toolkit, the online portal, is on the horizon. Working with a Mozilla-Ford Open Web Fellow, we have started to build the interactive portal. This website will help companies create and publish reports in a format that utilizes best practices, help researchers translate existing reports into a standardized format, and help consumers of these reports make the best use of the data.

**STARTING A DISCUSSION**

Over the past two years we have synthesized the various dialogues from our interviews and convenings and additional research into a document that surveys current practices and identifies the best practices of existing transparency reports. There is such a vast array of approaches and practices within current transparency reports that is impossible to address all questions or resolve all tensions. The *Transparency Reporting Toolkit*, including these *Survey & Best Practice Memos* and the attendant *Reporting Guide and Template* (forthcoming), is our attempt to start the discussion.

*— Kevin Bankston, Ryan Budish, and Liz Woolery*

# QUICK LOOK: OVERVIEW OF THE SURVEY & BEST PRACTICE MEMOS

**How to Read the Memos**

- Each memo begins with "Best Practices" in reporting and the companies engaged in those practices.* Some memos also include a section on "Other Practices of Note," which highlights "Approaching Best Practices" (strong reporting practices, but ones that fall just short of best practices) and "Notable Practices" (innovative approaches to reporting). Finally, each memo includes a table of "Current Practices" in reporting covering all companies surveyed.^
- Companies are listed in alphabetical order throughout the memos, including in the Best Practices, Other Practices of Note, and Current Practices sections.
- Columns to the right of the company name are the heart of the survey and document each company's practices. The content of these columns comes *directly from each company's transparency report*. Aside from minor changes made for readability, we have not altered or edited the text from how it originally appeared in the transparency report.
- Bracketed and italicized content indicates a clarification or note. For example, we have added "*[#]*" and "*[%]*" to indicate whether a company is reporting data as a number or a percentage.
- This document is not intended to provide legal advice. It is merely a starting point in the much larger discussion about the present and future of strong transparency reporting.

** Memo #8 covers reporting on national security orders. Given that the passage of the USA FREEDOM Act in June 2015 will impact reporting on these orders, this memo only surveys Current Practices and does not identify Best Practices.*

*^ Due to cumulative length of legal process definitions from multiple companies, Memo #2 (Explaining Best Practices) contains only the full text for definitions identified as Best Practices or Approaching Best Practices.*

| MEMO | TOPIC |
|---|---|
| **Memo #1** | **Reporting on Different Legal Processes**<br><br>This memo, the first in the series, surveys how companies categorize the different legal processes (e.g, search warrants, subpoenas,) used by law enforcement and government officials to request user information. |

| MEMO | TOPIC |
| --- | --- |
| **Memo #2** | **Explaining Legal Processes**<br><br>This memo surveys how companies define or explain legal processes (e.g, search warrants, subpoenas) in their transparency reports. |
| **Memo #3** | **Reporting on the Subjects of Requests & How Users are Impacted**<br>This memo surveys how companies report on the subjects of requests and how users are impacted by requests. Specifically, this memo surveys the terms used to describe subjects of requests (e.g., users impacted, accounts affected, URLs identified). This memo also includes explanatory information from companies' transparency reports about what those terms mean. |
| **Memo #4** | **Reporting on the Legal Processes Required for User Information**<br><br>This memo surveys how companies report on the provision of user information in response to legal process requests. Specifically, this memo surveys what information will be supplied in response to each type of legal process. |
| **Memo #5** | **Explaining "Content" & "Non-Content"**<br><br>This memo surveys how companies describe the "content" and "non-content" of user communications on their platforms. |
| **Memo #6** | **Reporting on Outcomes & Compliance with Requests**<br><br>This memo surveys how companies report on responses to and / or compliance with requests. Also included are explanations from the companies' transparency reports about how and why they report compliance and response data. |
| **Memo #7** | **Reporting on User Notification**<br><br>This memo surveys how companies report on notification of users who are the subjects of legal process requests. Also included are explanations from the companies' transparency reports about how and why they report on user notification. |
| **Memo #8** | **Reporting on National Security Orders**<br><br>This memo, the final in the series, surveys how companies report on National Security Letters and Foreign Intelligence Surveillance Court orders. |

# TRANSPARENCY REPORTS BY U.S. INTERNET & TELECOM COMPANIES

More than 40 United States Internet and telecommunications companies are engaged in the practice of transparency reporting. Basic information about those reports – hyperlinks, date of most recent publication (prior to July 10, 2015), and the time period covered by that report – are listed below. These are the companies and transparency reports included in the Toolkit's eight-memo survey of reporting practices.

*All reports published prior to July 10, 2015*
*Key: ^ Date according to news reports | * Date according to company blog post, social media, or PR*

| COMPANY | TRANSPARENCY REPORT<br>*Most Recent Publication (prior to July 1, 2015)* | DATE PUBLISHED | QUARTERS COVERED |
|---|---|---|---|
| **Adobe** | Government Requests Transparency Report (Web) | 3/12/2015* | 2014 — Q1, Q2, Q3, Q4 (excluding Dec.) |
| **Amazon** | Information Request Report (PDF) | 6/12/2015^ | 2015 — Q1, Q2 (excluding June) |
| **AOL** | Transparency Report (Web) | 10/28/2014 | 2014 — Q1, Q2 |
| **Apple** | Report on Government Information Requests July 1 – Dec 30, 2014 (PDF)<br>Report History (Web) | 4/2015 | 2014 — Q3, Q4 |
| **AT&T** | Transparency Report (Web)<br>Transparency Report (PDF) | 1/2015 | 2014 — Q3, Q4 |
| **Automattic** | Transparency Report (Web) | 5/27/2015 | 2015 — Q1, Q2 |
| **Cheezburger** | 2014 Transparency Report (Web) | 2/5/2015 | 2014 — Q1, Q2, Q3, Q4 |

| COMPANY | TRANSPARENCY REPORT<br>*Most Recent Publication (prior to July 1, 2015)* | DATE PUBLISHED | QUARTERS COVERED |
|---|---|---|---|
| **Cisco** | Transparency Report (Web) | 4/17/2015 | 2014 — Q1, Q2, Q3, Q4 |
| **CloudFlare** | Transparency Report for the Second Half of 2014 (Web) | Unknown | 2014 — Q3, Q4 |
| **Comcast** | Transparency Report (PDF) | 2/5/2015* | 2014 — Q3, Q4 |
| **CREDO Mobile** | Transparency Report – Q1 2015 (Web) | 4/2/2015 | 2015 — Q1 |
| **DigitalOcean** | Transparency Report: Jan-Jun 2015 (PDF) | 5/12/2015 | 2015 — Q1, Q2 |
| **DreamHost** | 2014 Transparency Report (PDF) | 3/11/2015 | 2014 — Q1, Q2, Q3, Q4 |
| **Dropbox** | 2014 Transparency Report (Web) | 1/28/2015* | 2014 — Q3, Q4 |
| **Evernote** | Transparency Report (Web) | Unknown | 2014 — Q1, Q2, Q3, Q4 |
| **Facebook** | Global Governments Requests Report (Web) | 3/16/2015 | 2014 — Q3, Q4 |
| **GitHub** | 2014 Transparency Report (Web) | 4/16/2015 | 2014 — Q1, Q2, Q3, Q4 |
| **Google** | Transparency Report (Web) | 5/14/2015 | 2014 — Q3, Q4 |
| **Inflection** | Transparency Report 2014 (PDF) | 5/30/2015 | 2014 — Q1, Q2, Q3, Q4 |
| **Internet Archive** | Summary of Requests for User Data from US Law Enforcement for 2014 (Web) | Unknown | 2014 — Q1, Q2, Q3, Q4 |
| **Kickstarter** | Transparency Report 2014 (Web) | 4/8/2015 | 2014 — Q1, Q2, Q3, Q4 |

| COMPANY | TRANSPARENCY REPORT<br>*Most Recent Publication (prior to July 1, 2015)* | DATE PUBLISHED | QUARTERS COVERED |
|---|---|---|---|
| **LinkedIn** | Transparency Report (Web) | 1/28/2015* | 2014 — Q3, Q4 |
| **Lookout** | 2013 Transparency Report (Web)<br>Transparency @ Lookout (Web) | 9/24/2013* | 2013 — Q1, Q2, Q3, Q4 |
| **Mapbox** | Transparency Report (Web) | Unknown | Unknown |
| **Medium** | Transparency Report (Web) | 1/5/2015 | 2014 — Q1, Q2, Q3, Q4 |
| **Microsoft** | Law Enforcement Requests Report (Web)<br>Law Enforcement Requests Report 2014 (PDF) | 3/26/2015 | 2014 — Q3, Q4 |
| **Nest** | Transparency Report: Requests for Information (Web) | 6/17/2015 | Unknown |
| **Pinterest** | Transparency Report Archive (Web) | 3/8/2015 | 2014 — Q4 |
| **Reddit** | Transparency Report, 2014 (Web)<br>Transparency Report, 2014 (PDF) | 1/29/2015* | 2014 — Q1, Q2, Q3, Q4 |
| **Silent Circle** | March 2015 Transparency Report (Web) | 3/15/2015 | Through March 2015 |
| **Slack** | Transparency Report (Web) | 5/1/2015 | Though April 2015 |
| **Snapchat** | Transparency Report (Web) | 4/2/2015 | 11/1/2014 — 2/28/2015 |
| **Sonic** | 2014 Transparency Report (Web) | 3/26/2015 | 2014 — Q1, Q2, Q3, Q4 |
| **SpiderOak** | Transparency Report: January 1 through December 1, 2014 (Web) | 2/12/2015 | 2014 — Q1, Q2, Q3, Q4 |

| COMPANY | TRANSPARENCY REPORT<br>*Most Recent Publication (prior to July 1, 2015)* | DATE PUBLISHED | QUARTERS COVERED |
|---|---|---|---|
| **Sprint** | Sprint Corporation Transparency Report (PDF) | 1/2015 | 2014 — Q1, Q2, Q3, Q4 |
| **T-Mobile** | Transparency Report for 2013 and 2014 (Web) | 7/6/2015 | 2014 — Q1, Q2, Q3, Q4<br>2015 — Q1, Q2, Q3, Q4 |
| **Time Warner Cable** | Transparency Reporting (Web) | Unknown | 2014 — Q3, Q4 |
| **Tumblr** | Transparency (Web)<br>Tumblr Transparency Report, July to December 2014 (PDF) | 4/9/2015 | 2014 — Q3, Q4 |
| **Twitter** | Transparency Report (Web) | 2/9/2015* | 2014 — Q3, Q4 |
| **Verizon** | Transparency Report (Web)<br>Verizon's Transparency Report for the Second Half of 2014 (PDF) | 1/15/2015* | 2014 — Q3, Q4 |
| **Wickr** | Transparency Report (PDF) | 6/30/2015 | 2015 — Q2 |
| **Wikimedia Foundation** | Transparency Report (Web)<br>Transparency Report (Wiki) | 4/7/2015 | 2014 — Q3, Q4 |
| **Yahoo** | Transparency Report | 3/26/2015^ | 2014 — Q3, Q4 |

# A BRIEF INTRODUCTION TO U.S. LAW ON GOVERNMENT ACCESS TO COMMUNICATIONS DATA

**ELECTRONIC COMMUNICATIONS PRIVACY ACT**

The federal law that regulates law enforcement access to customer data and content is the **Electronic Communications Privacy Act, or ECPA** (18 U.S.C. § 2510 et seq.). ECPA is made up of three component statutes: the Stored Communications Act (18 U.S.C. § 2701 et seq.), the Wiretap Act (18 U.S.C. § 2511 et seq.), and the Pen Register Statute (18 U.S.C. §3121 et seq.).

Each statute regulates government access to a variety of types of information regarding an Internet or telecommunications customer or subscriber. This information is described as **content** (of communications) and **non-content** (the data about those communications). Non-content data includes transactional data such as who a communication was to or from, the time it was transmitted, and the duration or size of the communication. Non-content also includes basic subscriber information such as a customer's name, address, billing information, and any subscriber identifier such as a username, email address, or IP address.

**1)** The **Stored Communications Act** (18 U.S.C. § 2701 et seq.) regulates the government's **retrospective** access to stored data — both the **content** of communications that have already happened and **non-content** data about those communications. The SCA is notoriously complex, but when read in conjunction with recent court rulings about how the Fourth Amendment applies to stored communications, the policy of most major companies is to require that the government provide:

- a **search warrant** for access to stored communications content (a search warrant is a court order based on a showing of probable cause, which means that there is "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."]
- a **subpoena** for access to basic subscriber information or to non-content transactional data about telephone calls (a subpoena is a legal demand issued directly by a prosecutor to a company without prior court approval and based on the prosecutor's determination that the material sought is relevant to a criminal investigation).
- a **court order under 18 U.S.C. §2703(d)** of the Stored Communications Act, often known as a "D Order," for any other non-content transactional records (a D Order is issued by the court 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).
- Companies also may voluntarily provide information in response to an **emergency request** in cases

where they have a good faith belief that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.

**2)** The **Wiretap Act** (18 U.S.C. § 2511 et seq.), sometimes known as "Title III," governs the interception or collection of the **content** of a target's **prospective** or "real-time" communications. A wiretap order is essentially a search warrant with special additional features unique to wiretaps. For example, wiretap orders can only be obtained for specific serious crimes, can only last 30 days unless renewed by the court, and require the government to "minimize" the interception of anything not relevant to the investigation.

**3)** The **Pen Register Statute** (18 U.S.C. §3121 et seq.), governs the use of so-called "pen registers" and "trap and trace devices" to capture **prospective** or "real-time" **non-content** information about a target's communications, such as information indicating who the communication was to or from, the time it was transmitted, and the duration or size of the communication. Pen register orders are issued by courts based on a very low standard, similar to that for a subpoena.

**CONTENT VS. NON-CONTENT INFORMATION**

| | **Retrospective** | | | | **Prospective (or "Real Time")** | |
|---|---|---|---|---|---|---|
| | **Stored Communications Act** | | | | **Wiretap Act** | **Pen Register Statute** |
| | *Search Warrant* | *Subpoena* | *D Order* | *Emergency Request* | *Wiretap Order* | *Pen Register Order* |
| **Content** | ✓ | | | ✓ | ✓ | |
| **Non-Content Transactional Information** | ✓ | | ✓ | ✓ | | ✓ |
| **Non-Content Subscriber Information** | ✓ | ✓ | ✓ | ✓ | | ✓ |

Whether customer information is content or non-content is not always straightforward. Often, an analogy from the pre-Internet world is used to help explain the distinction: Non-content information is similar to the information you find on the outside of an envelope, while content is the information found in a letter inside the envelope. The non-content information, such as the sender's name and address and the recipient's name and address, is on the outside of the "envelope," while the content of the communication, the "letter," remains inside. The analogy is not perfect. The content/envelope distinction was born during a series of mid-1970s privacy cases before the U.S. Supreme Court, and does not always analogize well to electronic or digital communications. The ECPA provides some clarity about how content and non-content are to be understood with respect to electronic communications:

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

**NATIONAL SECURITY ORDERS**

The Stored Communications Act also authorizes National Security Letters (18 U.S.C. §2709), secret subpoenas for certain basic subscriber and transactional information that prosecutors can use to demand information they determine is relevant to an anti-terrorism or espionage investigation. Another statute, the Foreign Intelligence Surveillance Act or FISA (50 U.S.C. §1801 et seq.), authorizes the specialized FISA Court to issue a variety of court orders for a wide range of surveillance and access to data, analogous to the variety of orders issued under ECPA for criminal cases but with much lower standards of proof and much more stringent secrecy requirements.

**RESTRICTIONS ON REPORTING ON REQUESTS FOR INFORMATION**

In transparency reports, companies often report the specific number of each type of ECPA legal process received, without any restrictions. However, when companies report on national security orders, they must do so using ranges. Prior to January 2014, companies were not permitted to report on national security orders whatsoever, as they are accompanied by a non-disclosure (or "gag") order. Following a January 2014 settlement with the U.S. Department of Justice,[1] companies party to the settlement were permitted to report on these orders using either a range of 0-249 or 0-999 (depending on whether the NSLs and FISA orders were counted in aggregate or separately). Following passage of the USA FREEDOM Act, all companies now have four options for reporting on national security orders. For specifics, see *Memo #8: Reporting on National Security Orders.*

[1] Settlement agreement letter available at http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf

# SURVEY & BEST PRACTICE MEMOS

# MEMO 1: REPORTING ON DIFFERENT LEGAL PROCESSES

# BEST PRACTICES

## FOR REPORTING ON DIFFERENT LEGAL PROCESSES

Reports from AT&T, Comcast, Facebook, Google, Sprint, T-Mobile, Time Warner Cable, and Verizon demonstrate the **best practice of clear and granular categorization of ECPA legal processes**.

An ideal report will, at minimum, provide the number of government requests for each the following processes, individually: search warrants, subpoenas, other court orders (e.g., 18 U.S.C. § 2703(d) orders), wiretap orders, pen register orders, and emergency requests. Each company reports request data on a process-by-process basis. Although the terminology is sometimes different (e.g., emergency requests vs. emergency disclosures), the granularity of reporting by these companies should be adopted as a standard for reporting on different legal processes.

In addition to reporting on specific legal processes, several companies (Facebook, Google, and Verizon) all report an aggregate number of requests received. AT&T and Comcast also report an aggregate number of requests, but exclude emergency requests from the total.

Moreover, such granular reporting of ECPA processes appears to be the minimum for these companies, as some report additional information. For example, AT&T's report breaks down criminal and civil subpoenas, Comcast's report breaks down search warrants into those for content vs. those for non-content, Google reports on the number of preservation requests received, and AT&T and Sprint both report on real-time location information.




*AT&T*'s report includes subpoenas (criminal, civil), court orders (historic, real-time), historic search warrants (stored content, other), real-time search warrants (wiretaps, mobile location demands), emergency requests (911, exigent), and location demands (historic, real-time, cell tower).




*Comcast*'s report is nearly as granular, reporting on subpoenas, court orders (general orders vs. pen register/trap and trace), wiretaps, and warrants (content, non-content), and emergency requests.



With its 2014 reports *Facebook* introduced more granularity than in prior reports, reporting on these categories: search warrant, subpoena, emergency disclosures, court order (18 USC 2703(d)), court order (other), pen register/trap and trace, and Title III requests.

# BEST PRACTICES

## FOR REPORTING ON DIFFERENT LEGAL PROCESSES

*Google*, engaged in transparency reporting since 2010 and thus the longest-reporting company, reports on six processes: subpoenas, emergency disclosures, search warrants, pen register orders, other court orders, and wiretap orders.

*Sprint*, relatively new to transparency reporting, quickly took up the best practice of reporting all individual ECPA categories: subpoenas, court orders, search warrants, emergency requests, pen registers/trap and traces, wiretaps, as well as real-time location requests.

*T-Mobile*'s reporting on ECPA processes includes subpoenas, emergency requests/911 calls, court orders, warrants/search warrants, other, pen register/trap and trace orders, and wiretap orders.

*Time Warner Cable* reports on subpoenas, court orders, search warrants, Emergency Requests, pen register and trap and trace, and Title III requests. However, TWC does not define these legal processes, making it unclear what it might include in the catch-all "court orders" category.

*Verizon*'s approach resembles Comcast's. The telecommunications company reports on subpoenas, orders (general vs. pen registers / trap and trace vs. wiretap), warrants, and emergency requests.

# CURRENT PRACTICES

## FOR REPORTING ON DIFFERENT LEGAL PROCESSES

As the three "Current Practices" charts on the following pages demonstrate, different companies categorize the requests they receive in different ways. Approaches to categorization break down into three tiers:

- **Tier 1: Most Processes Reported Individually, Not in Aggregate**

  AT&T, Comcast, Facebook, Google, Sprint, T-Mobile, Time Warner Cable, and Verizon, for example, provide individual reporting on all categories of ECPA (search warrants, wiretap orders, pen register orders, D orders/court orders, subpoenas, and emergency requests). Such granular reporting of ECPA processes appears to be the minimum for these companies, as some report additional information (such as Comcast's practice of breaking down search warrants into those for content vs. those for non-content) or on other processes (such real-time location information, which AT&T and Sprint report).

- **Tier 2: Mix of Individual and Aggregate Process Reporting**

  Amazon, Twitter, and Tumblr, for example, report some of the legal process requests they receive individually, while other requests are reported in aggregate. For example, Twitter reports search warrants, subpoenas, and emergency requests individually, but combines pen register and D orders into a "Court Orders" category. Tumblr reports search warrants, subpoenas, and emergency requests individually, but combines D orders and other orders issued under "various U.S. federal and state laws" in aggregate under a "court order" category. Several other companies, including Automattic, CloudFlare, Dropbox, LinkedIn, Pinterest, Reddit, and the Wikimedia Foundation, also report requests with a similar mix of individual and aggregated processes. Notably, CloudFlare also reports pen register and wiretap orders individually.

- **Tier 3: Most Processes Reported in Aggregate, Not Individually**

  The third approach to categorizing legal processes involves companies reporting most processes in aggregate and not individually. For example, Apple, Microsoft, and Yahoo report as a single aggregate number for the following processes: search warrants, wiretap orders, pen register orders, D orders, subpoenas, or emergency requests.

Every company that provides some granular reporting for ECPA requests has categories for "search warrants" and "subpoenas." However, categorization and terminology around legal process requests differ widely between companies, and represents the clearest need for improvement and opportunity for standardization. Many companies have categories for "court orders," "general orders," or "other" requests, often covering a

differing range of orders or requests. Most of the time, the terms "court orders," "general orders," and "other orders" appear to reference (or at least include) D orders. In some cases, however, it is unclear whether these vaguely defined catch-all categories also include wiretap orders or pen register orders.

The "Current Practices" charts on the following pages do not include every company that has issued a transparency report. Some companies have transparency reporting processes duplicative of those mentioned above, others use methods that are unique and sometimes unclear, and others report having received no requests for user information at this point. However, these tables capture the vast majority of approaches to categorizing and reporting on different legal processes.

## Tier 1: Most Processes Reported Individually, Not in Aggregate (Examples)

| | at&t | Google | verizon |
|---|---|---|---|
| **Search Warrant** | "Warrants" | "Search Warrant" | "Warrants" |
| **Wiretap Order** | "Wiretaps" | "Wiretap Order" | "Wiretap Orders" |
| **Pen Register Order** | "Pen Registers" | "Pen Register Order" | "Pen Registers / Trap & Trace Orders" |
| **18 U.S.C. § 2703(d) Order** | "General Court Orders" | "Other Court Orders" | "General Orders" |
| **Subpoena** | "Subpoenas" | "Subpoena" | "Subpoenas" |
| **Emergency Request** | "Emergency Requests" | "Emergency Disclosures" | "Emergency Requests from Law Enforcement" |

## Tier 2: Mix of Individual and Aggregate Process Reporting (Examples)

| |  |  |  |
|---|---|---|---|
| **Search Warrant** | "Search Warrants" | "Search Warrant" | "Search Warrants" |
| **Wiretap Order** | "Other Court Orders" | "Court Order" | "Court Orders"<br>*Notes % of these that are Pen Registers* |
| **Pen Register Order** | | | |
| **18 U.S.C. § 2703(d) Order** | | | |
| **Subpoena** | "Subpoenas" | "Subpoena" | "Subpoenas" |
| **Emergency Request** | *Does Not Report This Process* | "Emergency Request" | "Emergency Requests" |

## Tier 3: Most Processes Reported in Aggregate, Not Individually (Examples)

| |  | Microsoft | YAHOO! |
|---|---|---|---|
| **Search Warrant** | "Law Enforcement Account Requests" and "Law Enforcement Device Requests" | "Law Enforcement Requests" | "Criminal Government Data Requests" |
| **Wiretap Order** | | | |
| **Pen Register Order** | | | |
| **18 U.S.C. § 2703(d) Order** | | | |
| **Subpoena** | | | |
| **Emergency Request** | | | |

# MEMO 2: EXPLAINING LEGAL PROCESSES

# BEST PRACTICES

## FOR EXPLAINING LEGAL PROCESSES

Reports from Google and Verizon demonstrate the **best practice of clear and comprehensive explanations of legal processes.** Reports from AT&T and Comcast demonstrate "Approaching Best Practices," identified on the following page. Approaching Best Practices recognize reporting that falls just short of the best practices standard(s) but is nonetheless deserving of recognition for a demonstrated commitment to informative and comprehensive transparency reporting.

Defining legal processes and other key terms that appear in a transparency report is an overlooked — but key — part of the report. Few companies define or explain to readers all of the different types of legal processes they receive, although most explain at least some of the processes. While many readers of reports may be well-versed in legal terminology, there are readers who are unfamiliar with the legal processes or sources of law that appear in these reports, which is why **including definitions and/or explanations is in itself a best practice**.

Definitions or a glossary explaining legal processes and other key terms used in the report can inform readers about the types of process 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 process (particularly in more nebulous categories like "court orders").

Google

*Google* has the most granular and complete definitions for each category of legal process, including national security orders. Google defines each process and includes information on the company's process for handling and responding to law enforcement requests.

verizon

*Verizon*'s definitions are less detailed, but they are well-integrated into the design of the main report page (and available on a separate FAQ page). Verizon also includes information about how a request is authorized and how the company responds to requests.

# OTHER PRACTICES OF NOTE

FOR EXPLAINING LEGAL PROCESSES

## APPROACHING BEST PRACTICES

"Approaching Best Practices" are strong reporting practices, but ones that could benefit from additional information or granularity. Companies with these practices have demonstrated a clear commitment to informative and comprehensive explanations of legal processes, but fell just short of inclusion in "Best Practices."




*AT&T*'s definitions are accessible to lay readers and provide information about how specific legal process orders are authorized. For example, AT&T notes which orders require approval by a judge and which do not. However, AT&T's definitions lack the granularity of Google's and Verizon's. AT&T does not definite wiretap or pen register orders individually, instead, these definitions are incorporated under "General Court Orders" and "Search Warrants and Probable Cause Court Orders" sections.




*Comcast*'s definitions are straightforward, accessible, and easy to find (the company includes definitions for all legal process categories immediately below its reported data). However, Comcast's definitions could benefit from additional detail about the specific types of information to which the company has access and may be required to turn over.

# QUICK LOOK: HOW COMMON ARE LEGAL PROCESS DEFINITIONS?

| LEGAL PROCESS | WHICH COMPANIES DEFINE THIS PROCESS | # OF COMPANIES |
|---|---|---|
| National Security (NSLs & FISA) Orders | Amazon, Apple, AT&T, Automattic, Cisco, CloudFlare, Comcast, CREDO Mobile, DigitalOcean, Dropbox, Evernote, Facebook, GitHub, Google, Kickstarter, LinkedIn, Medium, Microsoft, Pinterest, Reddit, Sprint, Tumblr, Verizon, Wikimedia Foundation, Yahoo | 25 |
| Search Warrant | Amazon, AT&T, Automattic, Cheezburger, CloudFlare, Comcast, DigitalOcean, Dropbox, Facebook, GitHub, Google, LinkedIn, Reddit, Sprint, Tumblr, Twitter, Verizon, Wikimedia Foundation | 18 |
| Subpoena | Amazon, AT&T, Automattic, Cheezburger, CloudFlare, Comcast, Dropbox, DigitalOcean, Facebook, GitHub, Google, LinkedIn, Reddit, Sprint, Tumblr, Twitter, Verizon, Wikimedia Foundation | 18 |
| General and Other Court Orders | Amazon, AT&T, Automattic, CloudFlare, Comcast, DigitalOcean, Dropbox, Facebook, GitHub, Google, LinkedIn, Sprint, Tumblr, Twitter, Verizon, Wikimedia Foundation | 16 |
| Emergency Request | AT&T, Automattic, Cheezburger, Comcast, DigitalOcean, Facebook, Google, Reddit, Sprint, Twitter, Verizon | 11 |
| Pen Register Order | AT&T, CloudFlare, Comcast, DigitalOcean, Facebook, Google, Sprint, Twitter, Verizon | 9 |
| Wiretap Order | CloudFlare, Comcast, DigitalOcean, Facebook, Google, Sprint, Verizon | 7 |

# CURRENT PRACTICES

## FOR EXPLAINING LEGAL PROCESSES

Effective standardization of categories will also require effective standardization of definitions. Before standardizing, we should review how terms are currently being defined and identify the best practice. For those companies that granularly categorize and define different types of legal process, these are the these are the definitions that they use.

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **SEARCH WARRANT** | |
| **Google** *Search Warrant* | An order issued by a judge under ECPA based on a demonstration of probable cause that compels the production of information.<br><br>The threshold is higher still [compared to an ECPA Court Order] for an ECPA search warrant. To obtain one, a government agency must make a request to a judge or magistrate and meet a relatively high burden of proof: demonstrating "probable cause" to believe that contraband or certain information related to a crime is presently in the specific place to be searched. A warrant must specify the place to be searched and the things being sought. It can be used to compel the disclosure of the same information as an ECPA subpoena or court order—but also a user's search query information and private content stored in a Google Account, such as Gmail messages, documents, photos and YouTube videos. An ECPA search warrant is available only in criminal investigations. |
| **Verizon** *Warrant* | To obtain a warrant a law enforcement officer must show a judge that there is "probable cause" to believe that the evidence sought is related to a crime. This is a higher standard than the standard for a general order. Approximately two-thirds of the warrants we received in the second half of last year sought location information, stored content [such as text message content or email content] or both.<br><br>What showing must law enforcement make to obtain a warrant? To obtain a warrant a law enforcement officer has to show a judge that there is probable cause to believe that the evidence it seeks is related to a crime and in the specific place to be searched. |
| **AT&T** *Search Warrants and Probable Cause Court Orders* | Search Warrants and Probable Cause Court Orders are signed by a judge, and they are issued only upon a finding of "probable cause." To be issued, the warrant or order must be supported by sworn testimony and sufficient evidence to believe the information requested is evidence of a crime. Probable cause is viewed as the highest standard to obtain evidence. Except in emergency circumstances, a search warrant or probable cause court order for all real-time location information [i.e., wiretaps and GPS] and stored content [i.e., text and voice messages] is required for all jurisdictions, courts, and agencies. |

*--- Continued on next page ---*

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **AT&T**<br>*Search Warrants and Probable Cause Court Orders*<br><br>(Cont'd) | Our Location Demands category breaks out the number of court orders and search warrants we received by the type of location information (historical and real-time) they requested. We also provide the number of requests we received for cell tower searches, which ask us to provide all telephone numbers registered to a particular cell tower for a certain period of time (or to confirm whether a particular telephone number registered on a particular cell tower at a given time). We do not keep track of the number of telephone numbers provided to law enforcement in connection with cell tower searches. A single cell tower demand may cover multiple towers. Beginning with our last report, we are disclosing both the total numbers of demands and the total number of cell tower searches. For instance, if we received one court order that included ID numbers for two cell towers, we count that as one demand for two searches. For the 692 cell tower demands during this period, we performed 1,839 searches. We also maintain a record of the average time period that law enforcement requests for one cell tower search, which was 2 hours, 33 minutes for this reporting period. |
| **Comcast**<br>*Warrants* | Warrants typically seek information similar to that available under subpoenas and some court orders, but may also seek the contents of communications in certain cases. A judge signs a warrant based on a showing by the law enforcement entity seeking it that there is probable cause that the information sought by the warrant is evidence of a crime. |
| **SUBPOENA** | |
| **Google**<br>*Subpoena* | A formal request issued under ECPA for the production of information that may not involve a judge.<br><br>Of the three types of ECPA legal process for stored information, the subpoena has the lowest threshold for a government agency to obtain. In many jurisdictions, including the federal system, there is no requirement that a judge or magistrate review a subpoena before the government can issue it. A government agency can use a subpoena to compel Google to disclose only specific types of information listed in the statute. For example, a valid subpoena for your Gmail address could compel us to disclose the name that you listed when creating the account, and the IP addresses from which you created the account and signed in and signed out (with dates and times). Subpoenas can be used by the government in both criminal and civil cases. On its face, ECPA seems to allow a government agency to compel a communications provider to disclose the content of certain types of emails and other content with a subpoena or an ECPA court order (described below). But Google requires an ECPA search warrant for contents of Gmail and other services based on the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable search and seizure. |
| **Verizon**<br>*Subpoena* | We are required by law to provide the information requested in a valid subpoena. The subpoenas we receive are generally used by law enforcement to obtain subscriber information or the type of information that appears on a customer's phone bill. We continue to see that approximately half of the subpoenas we receive seek only subscriber information: that is, those subpoenas typically require us to provide the name and address of a customer assigned a given phone number or IP address. Other subpoenas also ask for certain transactional information, such as phone numbers that a customer called. The types of information we can provide in response to a subpoena are limited by law. We do not release contents of communications (such as text messages or emails) or cell site location information in response to subpoenas. |

*--- Continued on next page ---*

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **Verizon**<br>*Subpoena*<br><br>(Cont'd) | Does a law enforcement officer need to go before a judge to issue a subpoena? Under federal law and the law in many states the government does not need judicial approval to issue a subpoena. A prosecutor or law enforcement official may issue a subpoena to seek evidence relevant to the investigation of a possible crime.<br><br>Are there limits on the types of data law enforcement can obtain through a subpoena? Yes, in response to a subpoena, we only release the six types of information specifically identified in section 2703(c)(2)(A)-(F) of Title 18 of the United States Code: customer name, address, telephone or other subscriber number, length of service, calling records and payment records. Some states have stricter rules. We do not release any content of a communication in response to a subpoena.<br><br>Are there different types of subpoenas? Yes, we may receive three different types of subpoenas from law enforcement: a grand jury subpoena (the subpoena is issued in the name of a grand jury investigating a potential crime); an administrative subpoena (generally, a federal or state law authorizes a law enforcement agency to issue a subpoena); or a trial subpoena (the subpoena is issued in the name of the court in anticipation of a trial or hearing). |
| **AT&T**<br>*Subpoena* | Subpoenas don't usually require the approval of a judge and are issued by an officer of the court, i.e., an attorney. They are used in both criminal and civil cases, typically to obtain testimony or written business documents such as calling records and basic subscriber information such as the name and address listed on the billing account. |
| **Comcast**<br>*Subpoena* | Subpoenas typically seek basic customer account information that is contained in the business records of a service provider. Frequently, subpoenas seek the identification of a customer account by name and address based on a telephone number or Internet Protocol address assigned to the account. An officer of the court, such as a law enforcement officer or a prosecuting attorney, for example, usually signs a subpoena. |
| **WIRETAP ORDER** | |
| **Google**<br>*Wiretap Order* | An order issued by a judge under ECPA for real-time disclosure of content.<br><br>A wiretap order requires a company to hand over information that includes the content of communications in real-time. Of all the government requests than can be issued under ECPA, wiretap orders are the hardest to obtain. To satisfy legal requirements, a government agency must demonstrate that: a) someone is committing a crime listed 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. The court must also find that 'normal' ways to investigate crime have failed (or probably would fail), or are too dangerous to attempt in the first place. There are limits on how long a wiretap can run and requirements to notify users who have been tapped. |

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **Verizon**<br>*Wiretap Order* | A wiretap order is an order that requires a wire or electronic communications provider to provide access to the content of communications in real¬time to law enforcement. The order can relate to the content of telephone or Internet communications.<br><br>What are the different showings that law enforcement has to make for the different orders? A wiretap order is the most difficult for law enforcement to obtain. Under the law, law enforcement may not obtain a wiretap order unless a judge finds that there is probable cause to believe that an individual is committing one of certain specified offenses and that particular communications concerning that offense will be obtained through the wiretap. A wiretap order is only issued for a specified time.<br><br>A small subset ... of the orders we received ... required us to provide access to data in realtime ... we are required to assist with wiretaps, where law enforcement accesses the content of a communication as it is taking place. |
| **AT&T**<br>*Search Warrants and Probable Cause Court Orders* | Search Warrants and Probable Cause Court Orders are signed by a judge, and they are issued only upon a finding of "probable cause." To be issued, the warrant or order must be supported by sworn testimony and sufficient evidence to believe the information requested is evidence of a crime. Probable cause is viewed as the highest standard to obtain evidence. Except in emergency circumstances, a search warrant or probable cause court order for all real-time location information (i.e., wiretaps and GPS) and stored content (i.e., text and voice messages) is required for all jurisdictions, courts, and agencies. |
| **Comcast**<br>*Wiretap Orders* | Wiretap Orders seek real time access to the contents of communications. |

## PEN REGISTER ORDER

| | |
|---|---|
| **Google**<br>*Pen Register Order* | An order issued under ECPA for real-time disclosure of dialing, routing, addressing and signaling information, but not content.<br><br>A pen register or trap and trace order requires a company to hand over information about a user's communications (excluding the content of communications themselves) in real-time. With such an order, a government can obtain "dialing, routing, addressing and signaling information." This could include the numbers you dial on your phone to reach someone or an IP address issued by an ISP to a subscriber. It's easier for a government agency to get a pen register or trap and trace order than a wiretap orders or search warrant. To obtain one, the requesting agent has to certify that information likely to be obtained will be "relevant to an ongoing criminal investigation." Google believes this standard is too low, and has been working with the Digital Due Process coalition to make sure the court has a meaningful role in determining when these orders are issued. |

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **Verizon** *Pen Registers/ Trap & Trace Orders* | A pen register order requires us to provide law enforcement with real-time access to phone numbers as they are dialed, while a trap and trace order compels us to provide law enforcement with real-time access to the phone numbers from incoming calls. We do not provide any content in response to pen register or trap and trace orders.<br><br>A small subset ... of the orders we received ... required us to provide access to data in real-time. A pen register order requires us to provide law enforcement with real-time access to phone numbers as they are dialed, while a trap and trace order compels us to provide law enforcement with real-time access to the phone numbers from incoming calls. We do not provide any content in response to pen register or trap and trace orders ... generally a single order is for both a pen register and trap and trace.<br><br>What is a pen register or trap and trace order? Pen register or trap and trace orders require a wire or electronic communications provider (like Verizon) to afford access to "dialing, routing, addressing or signaling information." With a pen register order we must afford real-time access to the numbers that a customer dials (or IP addresses that a customer visits); with a trap and trace order we must afford real-time access to the numbers that call a customer. Such orders do not authorize law enforcement to obtain the contents of any communication.<br><br>What are the different showings that law enforcement has to make for the different orders? A pen register order or trap and trace order requires law enforcement to make a lesser showing [than a wiretap or general order] -- that the information likely to be obtained is relevant to an ongoing criminal investigation. |
| **AT&T** *General Court Orders* | General Court Orders are signed by a judge. We consider "general" court orders as all orders except those that contain a probable cause finding. In a criminal case, for example, a judge may issue a court order on a lesser standard than probable cause, such as "relevant to an ongoing criminal investigation." In a civil case, a court order may be issued on a "relevant" or "reasonably calculated to lead to the discovery of admissible evidence" standard. For this report, general court orders were used to obtain historical information like billing records or the past location of a wireless device. In criminal cases, they are also used to obtain real-time, pen register/"trap and trace" information, which provides phone numbers and other dialed information for all calls as they are made or received from the device identified in the order. |
| **Comcast** *Pen Register Orders* | Pen Register Orders seek real time access to information like phone numbers and e-mail addresses as they are dialed or sent, and Trap and Trace Orders seek real time access to incoming phone numbers or e-mail addresses. |
| **EMERGENCY REQUEST** | |
| **Google** *Emergency Disclosures* | A request from a government agency seeking information to save the life of a person who is in peril or prevent serious physical injury. |

*--- Continued on next page ---*

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **Google** *Emergency Disclosures* [Cont'd] | Sometimes we voluntarily disclose user information to government agencies when we believe that doing so is necessary to prevent death or serious physical harm to someone. The law allows us to make these exceptions, such as in cases involving kidnapping or bomb threats. Emergency requests must contain a description of the emergency and an explanation of how the information requested might prevent the harm. Any information we provide in response to the request is limited to what we believe would help prevent the harm. |
| **Verizon** *Emergency Request* | Law enforcement requests information from Verizon that is needed to help resolve serious emergencies. We are authorized by federal law to provide the requested information in such emergencies and we have an established process to respond to emergency requests, in accordance with the law. To request data during these emergencies, a law enforcement officer must certify in writing that there was an emergency involving the danger of death or serious physical injury to a person that required disclosure without delay. These emergency requests are made in response to active violent crimes, bomb threats, hostage situations, kidnappings and fugitive scenarios, often presenting life-threatening situations. In addition, many emergency requests are in search and rescue settings or when law enforcement is trying to locate a missing child or elderly person. We also receive emergency requests for information from Public Safety Answering Points (PSAPs) regarding particular 9-1-1 calls from the public. Calls for emergency services, such as police, fire or ambulance, are answered in call centers, or PSAPs, throughout the country. PSAPs receive tens of millions of calls from 9-1-1 callers each year, and certain information about the calls (name and address for wireline callers; phone numbers and available location information for wireless callers) is typically made available to the PSAP when a 9-1-1 call is made. Yet a small percentage of the time PSAP officials need to contact the telecom provider to get information that was not automatically communicated by virtue of the 9-1-1 call or by the 9-1-1 caller. |
| **AT&T** *Emergency Requests* | This category includes the number of times we responded to 911-related inquiries and "exigent requests" to help locate or identify a 911 caller. These are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies. The numbers provided in this category are the total of 911 and exigent searches that we processed during this reporting period. |
| **Comcast** *Emergency Requests* | Emergency Requests typically seek information from a service provider on an expedited basis in an emergency involving danger of death or serious physical injury to any person. Our policy requires the requesting law enforcement officer to provide a written certification describing the emergency. Comcast uses this information to verify an emergency request in connection with responding to it. Some emergency requests seek information related to 911 telephone calls. In those cases, Comcast verifies that the request is coming from a legitimate Public Service Answering Point before responding to it. |

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **NATIONAL SECURITY ORDERS** | |
| **Google** *National Security Letters and FISA Requests* | National Security Letters – [R]equests authorized by the FBI that can require U.S. companies to hand over "the name, address, length of service, and local and long distance toll billing records" of a subscriber for use in national security investigations. They don't require a court order and cannot be used to obtain anything else from Google, such as Gmail content, search queries, YouTube videos or user IP addresses.<br><br>What is a National Security Letter? It's a request for information that the Federal Bureau of Investigation (FBI) can make when they or other agencies in the Executive Branch of the U.S. government are conducting national security investigations. An NSL can't be used in ordinary criminal, civil or administrative matters. You can read more about NSLs in this publication by the Congressional Research Service [hyperlink omitted]. The FBI is required to report how they use NSLs to Congress biannually. The U.S. Department of Justice also regularly audits how the FBI uses NSLs.<br><br>What does an NSL compel Google to disclose? Under the Electronic Communications Privacy Act (ECPA) 18 U.S.C. section 2709, the FBI can seek "the name, address, length of service, and local and long distance toll billing records" of a subscriber to a wire or electronic communications service. The FBI can't use NSLs to obtain anything else from Google, such as Gmail content, search queries, YouTube videos or user IP addresses.<br><br>What process must the FBI follow to issue an NSL? The Director of the FBI or a senior FBI designee 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." The FBI is not required to get court approval to issue an NSL.<br><br>FISA Requests – [FISA] requests are orders that can require U.S. companies to hand over personal information in national security investigations.<br><br>*Google also publishes an extensive FAQ regarding national security requests. Excerpts are below.*<br><br>What is the 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. It also created the Foreign Intelligence Court of Review, to which appeals from the FISC can be made. These courts have the power to require companies or other private organizations to hand over information in foreign intelligence investigations. The Department of Justice 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. You can read more about FISA in these publications by the Congressional Research Service: February 15, 2007 CRS Report, July 7, 2008 CRS Report [hyperlink omitted].<br><br>What does a FISA request compel Google to disclose? Under the Foreign Intelligence Surveillance Act (FISA), the government may apply for court orders from the FISA Court to, among other actions, require U.S. companies to hand over users' personal information and the content of their communications. |

*--- Continued on next page ---*

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **Google**<br>*National Security Letters and FISA Requests*<br><br>(Cont'd) | The FISA Amendments Act, passed in 2008, authorizes the government 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. You can read more about the FISA Amendments Act in this publication by the Congressional Research Service: April 8, 2013 CRS Report.<br><br>If Google were to receive a FISA request, what would it do? Google's general approach to government requests for information is the same: Before complying with a government request, we make sure it follows the law and Google's policies. And if we believe a request is overly broad, we seek to narrow it.<br><br>What are the reporting delays imposed by the U.S. Department of Justice? The U.S. Department of Justice has imposed two delays. First, providers must wait six months before publishing statistics about FISA requests so that, for example, the report published January 1, 2015 will reflect requests received between January 1 and July 1, 2014. Second, providers must wait two years to publish statistics reflecting 'New Capability Orders.' |
| **Verizon**<br>*National Security Letter, or NSL and FISA Orders* | A National Security Letter, or NSL, is a request for information in national security matters; it cannot be used in ordinary criminal, civil or administrative matters. When the Director of the Federal Bureau of Investigation issues a National Security Letter to a wire or electronic communications provider (like Verizon) such a provider must comply. The law that authorizes the FBI to issue NSLs also requires the Director of the FBI to report to Congress regarding NSL requests.<br><br>Under what circumstances can the FBI issue an NSL? The FBI does not need to go to court to issue an NSL. Rather, the Director of the FBI or a senior designee must certify in writing that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.<br><br>What types of data can the FBI obtain through an NSL? The FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. The FBI cannot obtain other information from Verizon, such as content or location information, through an NSL.<br><br>In the second half of 2014, we received between 0 and 999 NSLs from the FBI. Those NSLs sought information regarding between 2000 and 2999 "selectors" used to identify a Verizon customer. (The government uses the term "customer selector" to refer to an identifier, most often a phone number, which specifies a customer. The number of selectors is generally greater than the number of "customer accounts." An NSL might ask for the names associated with two different telephone numbers; even if both phone numbers were assigned to the same customer account, we would count them as two selectors.) The FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. Verizon does not release any other information in response to an NSL, such as content or location information.<br><br>FISA Orders – A FISA order is an order issued by a judge of the Foreign Intelligence Surveillance Court. This Court was created by the Foreign Intelligence Surveillance Act of 1978 (commonly known as "FISA"). The FISA court considers requests by government agencies like the FBI or NSA to collect or conduct intelligence in the United States. The FISA court can issue an order compelling a private party, like Verizon, to produce intelligence information to the government. |

*--- Continued on next page ---*

| COMPANY | DEFINITION / EXPLANATION |
|---|---|
| **Verizon**<br>*National Security Letter, or NSL and FISA Orders*<br><br>(Cont'd) | What is a FISA order for content? A FISA order for content is an order that compels Verizon to give the government the content of certain communications carried on Verizon's networks. A FISA order for content could compel Verizon to intercept voice communications or provide the government with stored content.<br><br>What is a FISA order for non-content? A FISA order for non-content is an order that compels Verizon to produce call detail records or similar "transactional" information about communications carried on Verizon's networks, but does not require Verizon to produce any content. |
| **AT&T**<br>*National Security Demands* | Court orders issued pursuant to FISA may direct us to respond to government requests for content and non-content data related to national security investigations, such as international terrorism or espionage.<br><br>These types of demands have very strict policies governing our ability to disclose the requests. The recent "Statistical Transparency Report Regarding Use of National Security Authorities" published by the Director of National Intelligence on June 26, 2014, does not alter the Department of Justice's Jan. 27, 2014, guidance. |
| **Comcast**<br>*National Security Letters and Foreign Intelligence Surveillance Act Orders and Warrants* | National Security Letters are issued by the Federal Bureau of Investigation. The FBI issues these in connection with counter-terrorism or counter-intelligence matters; national security letters are limited to seeking non-content information like customer account information.<br><br>Foreign Intelligence Surveillance Act Orders and Warrants are issued by the Foreign Intelligence Surveillance Court. These orders and warrants typically seek both content and non-content information relating to national security matters, such as international terrorism or espionage. |

# MEMO 3: REPORTING ON THE SUBJECTS OF REQUESTS & HOW USERS ARE IMPACTED

# BEST PRACTICES

## FOR REPORTING ON THE SUBJECTS OF REQUESTS & HOW USERS ARE IMPACTED

Reports from Google, Snapchat, and Verizon collectively demonstrate the **best practice of granular reporting on the subjects of requests and how users are impacted.** The Wikimedia Foundation's report demonstrates "Notable Practices," identified on the following page. Notable Practices are innovative, unique, or noteworthy practices, but ones that may not be feasible for all companies.

There are two best practices for reporting on the subjects of requests: **The first best practice is to report the number of selectors specified in a request.** This includes all unique identifiers (e.g., name, phone number, email address). **The second best practice is to report the number of users and/or accounts responsive to a request.** These are users and/or accounts directly targeted by the selectors. Whether a company reports users vs. accounts depends on whether that company has a user- or account-based service (some companies may have both). Companies should be clear in their reports about whether they are reporting on users, accounts, or both. For example, a company may explain that a single user can have multiple accounts or that multiple users can share a single account.

No company employs both best practices, but reports from Google, Snapchat, and Verizon come closest.

Google

*Google* reports on the number of "users/accounts specified" in requests and provides a detailed explanation about what is included in that count. For example, Google states that this is "not the total number of users that have been the subject of a request," because the company errs on the side of over-inclusivity by, for example, including accounts that were requested in different legal processes.

*Snapchat* reports on selectors, although the company calls them "account identifiers." Snapchat also offers a detailed explanation of this term, noting that a single request could identify multiple selectors or that a single selector might be specified in multiple requests.

verizon

*Verizon* is the only other company reporting on selectors, which the company refers to as "information points." However, Verizon only reports on the selectors identified in subpoenas, not other processes.

# OTHER PRACTICES OF NOTE

FOR REPORTING ON THE SUBJECTS OF REQUESTS & HOW USERS ARE IMPACTED

## NOTABLE PRACTICES

"Notable practices" are innovative approaches to reporting. Notable practices may not be feasible for all companies, but for those with the resources and opportunity, they offer a chance to add additional transparency and information.

WIKIMEDIA FOUNDATION

The *Wikimedia Foundation* offers detailed definitions for the terms used to describe subjects of requests. Wikimedia reports on both the number of user accounts "potentially affected" and the number of user accounts "actually affected" and, in a FAQ, defines what each term means (see page 48).

# CURRENT PRACTICES

## FOR REPORTING ON THE SUBJECTS OF REQUESTS & HOW USERS ARE IMPACTED

The following table details the terms used by companies reporting on the subjects of requests for user information. The diversity of terms used to describe the subjects of these requests (e.g., whether the subject was an account, a website, or a user; whether the subject was targeted, specified, or affected) highlights one area of transparency reporting in need of standardization. Given that companies are reporting on different – albeit related – data points regarding the subjects of requests, the data across companies is incomparable, preventing readers from understanding the scale and scope of the U.S. government requests for user information received by U.S. Internet and telecommunications companies.

| COMPANY | SUBJECT (e.g., Users, Accounts) | ACTION REPORTED (e.g., Affected, Specified) | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Adobe** | Number of **users** | **Impacted** | |
| **Amazon** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **AOL** | Number of **Accounts** | **Affected** | |
| **Apple** | Number of **Devices** | **Specified** in the Requests | The total number of iPhone, iPad, iPod, Mac, or other devices identified in each law enforcement request, based on the number of device identifiers. For example, law enforcement agencies investigating theft cases often send requests seeking information based on serial numbers. Each serial number is counted as a single device. A request may involve multiple devices as in the case of a recovered shipment of stolen devices. |

*--- Continued on next page ---*

| COMPANY | SUBJECT (e.g., Users, Accounts) | ACTION REPORTED (e.g., Affected, Specified) | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Apple** (Cont'd) | Number of **Accounts** | **Specified** in the Requests | The number of discernible accounts, based on specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers in each law enforcement request. A single request may involve multiple accounts where, for example, multiple accounts are associated with the same credit card. |
| **AT&T** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Automattic** | Number of **sites** | **Specified** | We receive requests that don't properly identify a site or user, so the number of sites specified may otherwise be greater. |
| **Cheezburger** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Cisco** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **CloudFlare** | Total # of **domains** | **affected** | The Total # of domains affected and the Total # of accounts affected refer only to requests which have been answered. |
| | Total # of **accounts** | **affected** | |
| **Comcast** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **CREDO Mobile** | Number of customer **accounts** | **for which customer information was produced** | |
| **DigitalOcean** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **DreamHost** | Number of **Accounts** | **Affected** | Estimation based on accounts specified in initial requests |

| COMPANY | SUBJECT (e.g., Users, Accounts) | ACTION REPORTED (e.g., Affected, Specified) | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Dropbox** | **Accounts** | **listed** in warrants *(#)* | … we look at how many accounts are listed in each piece of legal process (whether a subpoena, search warrant, or court order). Some only identify a single account, whereas others identify tens of accounts in a single request. |
| | **Accounts** | **listed** in subpoenas *(#)* | |
| **Evernote** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Facebook** | **Users / Accounts** | **Requested** *(#)* | … requests for data about people who use Facebook … |
| **GitHub** | **Accounts** | **Affected** by Subpoenas, Court Orders, and Search Warrants *(#)* | Some requests may seek information about more than one account. |
| **Google** | **Users/Accounts** | **Specified** *(#)* | There may be multiple requests that ask for data for the same entity or a single request that specifies one or more entities.<br><br>… it's not the total number of users that have been the subject of a request to Google. There are several reasons why the numbers of "users/accounts" in user information requests may be over-inclusive. For example, the same Gmail account may be specified in several different requests for user information, perhaps once in a subpoena and then later in a search warrant. We add both instances to the "user/accounts" total even though it's the same account. Similarly, we might receive a request for a user or account that doesn't exist at all. In that case, we would still add both the request and the non-existent account to the totals. We've taken efforts to reduce over-inclusiveness, but have decided it is better to error on the side of a greater number. |
| **Inflection** | *Does not report on the subjects of requests and how users are impacted.* | | |

| COMPANY | SUBJECT (e.g., Users, Accounts) | ACTION REPORTED (e.g., Affected, Specified) | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Internet Archive** | **User accounts** | **targeted** *(#)* | |
| **Kickstarter** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **LinkedIn** | **Accounts** | **Subject to Request(s)** *(#)* | This column was previously labeled "Accounts Impacted", but we changed the name to clarify that it reflects the number of accounts subject to the data requests, and not the number of accounts for which some responsive data was in fact provided ... |
| | **Accounts** | **Impacted** (LI Provided Some Data) *(#)* | We started reporting the number of accounts for which at least some data was provided in response to government requests in our January-June 2014 transparency report. |
| **Lookout** | **User Accounts** | **Affected** *(#)* | |
| **Mapbox** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Medium** | *Does not report on the subjects of requests and how users are impacted.* | | |

| COMPANY | SUBJECT (e.g., Users, Accounts) | ACTION REPORTED (e.g., Affected, Specified) | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Microsoft** | **Accounts/Users** | **Specified** in Requests *(#)* | The total number of usernames, accounts, or other identifiers that were specified in the requests received. One law enforcement request could include the names of multiple users, and/or could include multiple accounts associated with a single user. For example, one user could have multiple accounts – such as an Outlook.com E-mail account, an Xbox Gamertag, a Microsoft Account ID, or an Xbox serial number.<br><br>Fewer users are impacted than the number of accounts impacted, but for a variety of reasons, it is difficult to determine an exact number. For example, a single request may seek information about multiple accounts belonging to one user or the same accounts may also be subject to repeat orders in different timeframes and, as a result, be "double counted". |
| **Nest** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Pinterest** | Number of **Accounts** | | |
| **Reddit** | # of **user accounts** | **named** in requests | |
| **Silent Circle** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Slack** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Snapchat** | **Account Identifiers** *(#)* | | "Account Identifiers" reflects the number of identifiers (e.g., username, email address, phone number, etc.) specified by law enforcement in legal process when requesting user information. Some legal process may include more than one identifier. In some instances, multiple identifiers may identify a single account. In instances where a single identifier is specified in multiple requests, each instance is included. |

| COMPANY | SUBJECT (e.g., Users, Accounts) | ACTION REPORTED (e.g., Affected, Specified) | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Sonic** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **SpiderOak** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Sprint** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **T-Mobile** | *Does not report on the subjects of requests and how users are impacted.* | | |
| **Time Warner Cable** | **Users/Accounts** *(#)* | | |
| **Tumblr** | # of **URLS** | **Affected** *(#)* | … Tumblr URLs. |
| **Twitter** | **Accounts** | **specified** *(#)* | … number of accounts affected by [government requests.<br><br>'Accounts specified' includes Twitter and Vine accounts identified in government requests we have received.<br><br>The number may include duplicate accounts or requests for accounts that do not exist or were misidentified. |
| **Verizon** | **information points** *(also referred to as **selectors**)* | **sought** *[in subpoenas] (#)* | … information points, such as a telephone number, used to identify a customer.<br><br>The number of selectors is usually greater than the number of customer accounts: if a customer had multiple telephone numbers, for instance, it's possible that a subpoena seeking information about multiple selectors was actually seeking information about just one customer. |
| **Wickr** | **Accounts** | **Associated** *(#)* | |

| COMPANY | SUBJECT (e.g., Users, Accounts) | ACTION REPORTED (e.g., Affected, Specified) | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Wikimedia Foundation** | **User Accounts** | **Potentially Affected** *(#)* | This number represents the number of unique user accounts implicated by requests for user data and whose data would have been disclosed if we had granted every request we received. This number may not reflect the number of unique individuals implicated by requests for user data; if an individual has multiple accounts across all Wikimedia projects, and we receive requests for more than one of these accounts, we record each user account separately. As a result, this number might overestimate the number of individuals implicated by user data requests. |
| | **User Accounts** | **Actually Affected** *(#)* | This number represents the number of unique user accounts whose nonpublic information was disclosed as a result of WMF receiving a valid request for user data. This number may not reflect the number of unique individuals whose data was disclosed as a result of a valid request for user data; if an individual has multiple accounts across all Wikimedia projects, and we receive requests for more than one of these accounts, we record each user account separately. As a result, this number might overestimate the number of individuals implicated by user data requests. |
| **Yahoo** | Total **Government Specified Accounts** *(#)* | | Government Specified Accounts: The number of Yahoo accounts, users, or other unique identifiers listed in a Government Data Request. This number is typically larger than the number of users and accounts actually involved because: 1) a single account may be included in more than one Government Data Request; 2) an individual user may have multiple accounts that were specified in one or more Government Data Requests; and 3) if a Government Data Request specified an account that does not exist, that nonexistent account would nevertheless be included in our count of Government Specified Accounts. |

# MEMO 4: REPORTING ON THE LEGAL PROCESSES REQUIRED FOR USER INFORMATION

# BEST PRACTICES

## FOR REPORTING ON THE LEGAL PROCESSES REQUIRED FOR USER INFORMATION

Because readers of transparency reports may be unfamiliar with the intricacies of the U.S. legal system, it is important for companies to demonstrate the **best practice of informative explanations of the legal processes the company requires in order to turn over specific types of user information**. T-Mobile's approach to reporting this information demonstrates the best practice, while reports from AT&T, Automattic, and Reddit demonstrate "Approaching Best Practices," identified on the following page. Approaching Best Practices recognize reporting that falls just short of the best practices standard(s) but is nonetheless deserving of recognition for a demonstrated commitment to informative and comprehensive transparency reporting.

*T-Mobile* has the most thorough and detailed accounting of the legal processes the company requires in order to turn over specific types of user information. In a two-column table, T-Mobile details 10 different types of information and the corresponding legal process required for each. T-Mobile's reporting is straightforward and thorough and demonstrates informative reporting on legal processes required for the provision of user information.




**A second best practice is a statement in the transparency report that the company requires a warrant before producing user content**. Some companies follow the U.S. Court of Appeals for the Sixth Circuit's 2010 holding in *U.S. v. Warshak* (631 F.3d 266) that email content is protected by the Fourth Amendment and therefore the government must produce a warrant to access that content, even though ECPA allows for the provision of content *without* a warrant. Many companies have this policy, though few include it in their transparency report.[1] The companies that state they require a warrant for content in their transparency reports are: Apple, Automattic, Cheezburger, Dropbox, Evernote, Google, Inflection, Internet Archive, Microsoft,[2] Reddit, T-Mobile, Twitter, Verizon, and Wikimedia Foundation.

---

[1] *A number of other companies require a warrant for content, but do not state so in their transparency reports (instead, they state so elsewhere, such as in a law enforcement guide). These companies include Adobe, CloudFlare, Comcast, DigitalOcean, Facebook, GitHub, Kickstarter, LinkedIn, Lookout, Mapbox, Medium, Pinterest, Slack, Snapchat, Sonic, SpiderOak, Tumblr, and Yahoo.*

[2] *Microsoft states that the company has "implemented the holding of* U.S. v. Warshak*" (suggesting that a warrant is required for production of content), however, Microsoft separately states that they "require a court order or warrant before we will consider disclosing content to law enforcement."*

# OTHER PRACTICES OF NOTE

FOR REPORTING ON THE LEGAL PROCESSES REQUIRED FOR USER INFORMATION

## APPROACHING BEST PRACTICES

"Approaching Best Practices" are strong reporting practices, but ones that could benefit from additional information or granularity. Companies with these practices have demonstrated a clear commitment to informative and comprehensive reporting on the legal processes required for access to user information, but fell just short of inclusion in "Best Practices."




*AT&T* provides a clear statement of policy regarding production of user information in response to requests. AT&T's practice is especially notable for detailing the circumstances under which the company will provide call detail records and location information.




*Automattic* also provides a clear statement of policy regarding production of user information in response to requests. Automattic specifically details the circumstances under which the company will provide IP addresses, non-public content, and content.




*Reddit* also provides a clear statement regarding when and what information it will provide. Reddit's report explains the circumstances under which the company will share subscriber information and also explains what that information includes.

# CURRENT PRACTICES

## FOR REPORTING ON THE LEGAL PROCESSES REQUIRED FOR USER INFORMATION

Some, but not all, companies include information in their transparency reports about the specific legal processes (e.g., search warrant) required for certain types of user information (e.g, content). The table below highlights the statements of policy that companies include in their transparency reports about what legal process(es) they require in order to provide different types of user information. This includes statements that the company follows the holding in *U.S. v. Warshak* that a search warrant is required for user content.

| COMPANY | LEGAL PROCESS REQUIRED FOR [ TYPE OF CONTENT / DATA ] |
|---|---|
| **Adobe** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Amazon** | We produce **non-content information** only in response to valid and binding **subpoenas**. We do not produce content information in response to subpoenas.<br><br>We may produce **non-content and content information** in response to valid and binding **search warrants**. |
| **AOL** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Apple** | Any government agency demanding customer **content** from Apple must get a **search warrant**.<br><br>We ... only provide account **content** when the legal request is a **search warrant**. |
| **AT&T** | ... in some states we must supply **call detail records** if we receive a **subpoena**. In other states, **call detail records** require a **court order** or **search warrant**.<br><br>... we will reject a subpoena requesting a **wiretap**, because either a **probable cause court order** or **search warrant** is required.<br><br>Except in emergency situations, we require the most stringent legal standard — a **search warrant** or **probable cause court order** — for all demands for **specific location information**. |

*--- Continued on next page ---*

| COMPANY | LEGAL PROCESS REQUIRED FOR [ TYPE OF CONTENT / DATA ] |
|---|---|
| **AT&T**<br><br>(Cont'd) | The legal standard required for the production of **other location data** is unsettled. Under current law, the lower standard of a **general court order** ... often applies ...<br><br>... we require an **order signed by a judge** before producing any type of **location information** that the federal government requests. |
| **Automattic** | Except in emergencies ... it is our policy to turn over **private user information** only upon receipt of a valid **subpoena, search warrant, or US Court order** ...<br><br>If these pieces of information are available, we can provide the **first and last names, phone number, email address currently assigned to a site owner, the date/time stamped IP address from which a site was created, the physical address, and the PayPal transaction information** ... upon receipt of a valid **subpoena**.<br><br>Except in emergencies, we require a **court order or a warrant** before providing additional **IP addresses or information relating to a specific post or a specific comment**.<br><br>We require a **warrant** before disclosing **content of user communications** to government agencies/ law enforcement.<br><br>We also require a **warrant** before providing any **non-public content information** (such as private or draft post content, or pending comments).<br><br>Automattic will only provide **content information and user communications** to law enforcement/ government agencies pursuant to a **search warrant**. See **United States v. Warshak**, 631 F.3d 266, 288 (6th Cir. 2010).<br><br>Automattic does not produce content information in response to a **subpoena**, but does produce account data such as **username, email address, IP address, legal name, physical address, and payment records**, if provided. |
| **Cheezburger** | Cheezburger requires a **search warrant** to be approved by a judge and **based on probable cause** to disclose **user content information**, which includes private messages, images, links, and posts/ comments that have been deleted or otherwise hidden from public view. |
| **Cisco** | ... absent a valid **warrant or court order**, we will not provide any **customer data** to the U.S. government. |
| **CloudFlare** | CloudFlare follows the principles laid out in **U.S. v. Warshak** and requires a valid **search warrant** before disclosing any **customer content** sought by law enforcement. |
| **Comcast** | *Report does not disclose the legal process(es) required for specific types of user information.* |

| COMPANY | LEGAL PROCESS REQUIRED FOR [ TYPE OF CONTENT / DATA ] |
|---|---|
| **CREDO Mobile** | *Report does not disclose the legal process(es) required for specific types of information.* |
| **DigitalOcean** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **DreamHost** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Dropbox** | All requests for **content information** were accompanied by a **search warrant**, which is the legal standard that Dropbox requires.<br><br>In response to court orders, we will not produce **content information** unless the court order has procedural safeguards equivalent to those of a **search warrant**. |
| **Evernote** | We ... require a **search warrant** before considering the disclosure of the **contents of an Evernote account**. |
| **Facebook** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **GitHub** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Google** | Google requires an **ECPA search warrant** for **contents of Gmail and other services** based on the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable search and seizure. |
| **Inflection** | We require at least a valid **subpoena** issued under state or federal law in order to produce **customer registration information or transaction records**.<br><br>We require a **search warrant** based on probable cause in order to produce **user content and communications**. |
| **Internet Archive** | The Internet Archive requires a **search warrant** before disclosing to law enforcement the **contents of non-public user communications**. |
| **Kickstarter** | *Report does not disclose the legal process(es) required for specific types of user information.* |

| COMPANY | LEGAL PROCESS REQUIRED FOR [ TYPE OF CONTENT / DATA ] |
|---|---|
| **LinkedIn** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Lookout** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **MapBox** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Medium** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Microsoft** | We require a valid **subpoena or legal equivalent** before we consider releasing a customer's **non-content data** to law enforcement;<br><br>We require a court order or **warrant** before we consider releasing a customer's content data; ... |
| **Nest** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Pinterest** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Reddit** | reddit requires a **subpoena** if a government wants reddit to share **subscriber information**, which includes IP addresses, the date that an account was created and e- mail addresses.<br><br>reddit requires a **search warrant based on probable cause** to disclose **user content information**, which includes private messages and posts/comments that have been deleted or otherwise hidden from public view. |
| **Silent Circle** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Slack** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Snapchat** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Sonic** | *Report does not disclose the legal process(es) required for specific types of user information.* |

| COMPANY | LEGAL PROCESS REQUIRED FOR [ TYPE OF CONTENT / DATA ] |
|---|---|
| **SpiderOak** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Sprint** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **T-Mobile** | Information Type Requested: Subscriber Information (e.g., information a customer provides when signing up for service, such as name and address, and call detail information), Minimum Required Legal Process: Subpoena<br><br>Information Type Requested: Historical Call Detail Information (e.g., information about calls made in the past, such as start time, duration, numbers called), Minimum Required Legal Process: Subpoena<br><br>Information Type Requested: Emergency Information (e.g., location information, call detail, content, in emergencies), Minimum Required Legal Process: Certification from Law Enforcement/Public Safety Answering Points<br><br>Information Type Requested: Real Time Call Detail Information (e.g., information on incoming and outgoing phone numbers for a specific phone/mobile device), Minimum Required Legal Process: Pen Register Court Order<br><br>Information Type Requested: Real Time Audio (e.g., phone conversation), Minimum Required Legal Process: Wiretap Court Order<br><br>Information Type Requested: Real Time Content (e.g., text messages), Minimum Required Legal Process: Wiretap Court Order<br><br>Information Type Requested: Real Time Location (e.g., approximate location of a phone/mobile device), Minimum Required Legal Process: Warrant<br><br>Information Type Requested: Historical Cell Site Location Information (e.g., location of towers that a phone/mobile device used in the past over a specific period of time), Minimum Required Legal Process: Court Order or Warrant* (*Depends on the applicable jurisdiction.)<br><br>Information Type Requested: Historical Cell Tower Dump Information (e.g., list of phone numbers which used a specific tower during a specific period of time), Minimum Required Legal Process: Warrant<br><br>Information Type Requested: Stored Content (e.g., saved voicemail message), Minimum Required Legal Process: Warrant |
| **Time Warner Cable** | *Report does not disclose the legal process(es) required for specific types of user information.* |

| COMPANY | LEGAL PROCESS REQUIRED FOR [ TYPE OF CONTENT / DATA ] |
|---|---|
| **Tumblr** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Twitter** | A properly executed **warrant** is required for the disclosure of the **contents of communications** (e.g., Tweets, DMs). |
| **Verizon** | We require a **warrant** before disclosing **stored content** to law enforcement, absent an emergency involving the danger of death or serious physical injury.<br><br>Verizon only releases such **stored content** to law enforcement with a **probable cause warrant**; we do not produce stored content in response to a general order or subpoena.<br><br>Verizon only produces **location information** in response to a **warrant** or order. |
| **Wickr** | *Report does not disclose the legal process(es) required for specific types of user information.* |
| **Wikimedia Foundation** | For the avoidance of doubt, we believe a **warrant** is required by the 4th Amendment to the United States Constitution, which prohibits unreasonable search and seizure and overrides conflicting provisions in the ECPA. |
| **Yahoo** | *Report does not disclose the legal process(es) required for specific types of user information.* |

# MEMO 5: EXPLAINING “CONTENT” & “NON-CONTENT”

# BEST PRACTICES

## FOR EXPLAINING "CONTENT" AND "NON-CONTENT"

*Google*'s transparency report demonstrates the **best practice of explaining what "content" and "non-content" mean while also providing a non-exhaustive list of provider-specific examples.** Reports from Dropbox, Verizon, and Yahoo demonstrate "Approaching Best Practices," identified on the following page. Approaching Best Practices recognize reporting that falls just short of the best practices standard(s) but is nonetheless deserving of recognition for a demonstrated commitment to informative and comprehensive transparency reporting. Additionally, Cisco's report demonstrates "Notable Practices," also identified on the following page. Notable Practices are innovative, unique, or noteworthy practices, but ones that may not be feasible for all companies

While ECPA defines "content" and "non-content," it is important for companies to elaborate on those definitions so that readers might understand the significance of the information in the transparency report. Further, these statutory definitions are outdated and don't clearly fit in the landscape of today's Internet and telephone services. Companies should take the opportunity to explain how statutory definitions apply or don't apply to the variety of services offered. In the interest of protecting user privacy, many companies will not want to provide an exhaustive list of the available user information, which is why **the best practice is for companies to be detailed and illustrative, although not necessarily exhaustive**. Companies should include provider-specific descriptive examples of content and non-content.




*Google*'s report offers the most informative approach to explaining to users what content and non-content mean, and specifically, what those terms mean for users of the company's Gmail, YouTube, Google Voice, and Blogger services. Google includes examples of both content and non-content specific to each service, as well as general definitions or examples for both terms.

# OTHER PRACTICES OF NOTE

FOR EXPLAINING "CONTENT" AND "NON-CONTENT"

## APPROACHING BEST PRACTICES

"Approaching Best Practices" are strong reporting practices, but ones that could benefit from additional information or granularity. Companies with these practices have demonstrated a clear commitment to informative and comprehensive explanations of legal processes, but fell just short of inclusion in "Best Practices."

*Dropbox* has taken a simplistic but straightforward approach to explaining content and non-content, including short definitions for each term, but also highlighting examples of each that are specific to its service.

*Verizon* also has taken a straightforward approach, offering definitions for "stored content" and "non-content" with provider-specific examples. Verizon's definitions also integrate text from relevant statutes alongside non-legalese descriptions.

*Yahoo* defines both "content" and "NCD" [non-content data] in its report. For both terms the company includes easy-to-understand language along with multiple examples specific to its services, such as Flickr and Yahoo Answers.

## NOTABLE PRACTICES

"Notable practices" are innovative approaches to reporting. Notable practices may not be feasible for all companies, but for those with the resources and opportunity, they offer a chance to add additional transparency and information.

*Cisco* has taken a comprehensive approach to explaining non-content data. The company includes comprehensive definitions for four types of non-content data: administrative data, payment data, support data, and telemetry data.

# CURRENT PRACTICES

## FOR EXPLAINING "CONTENT" AND "NON-CONTENT"

Companies have taken a variety of approaches to explaining to users the information that might be provided in response to requests and, more specifically, to describing content and non-content. Some companies do not define these terms at all, others use the statutory language, others provide examples, and yet others do some combination of the statutory language and providing examples.

| COMPANY | CONTENT | NON-CONTENT |
|---|---|---|
| **Adobe** | *No definition / examples provided in report.* | |
| **Amazon** | "Content" information means the content of data files stored in a customer's account. | "Non-content" information means subscriber information such as name, address, email address, billing information, date of account creation, and certain purchase history and service usage information. |
| **AOL** | *No definition / examples provided in report.* | |
| **Apple** | ... content such as iCloud email, contacts, calendar, or Photo Stream content. | ... relevant device information, such as registration, subscriber, service, repair, and purchase information ...<br><br>... subscriber or transactional information ...<br><br>... iCloud, iTunes, or Game Center data ... |
| **AT&T** | ... stored content (i.e., text and voice messages) ...<br><br>... real-time location information ... | ... non-content information, such as a list of phone numbers dialed or subscriber information.<br><br>... call detail records ...<br><br>... calling records and basic subscriber information such as the name and address listed on the billing account.<br><br>... historical information like billing records or the past location of a wireless device. |

*--- Continued on next page ---*

| COMPANY | CONTENT | NON-CONTENT |
|---|---|---|
| **AT&T**<br><br>(Cont'd) | | ... phone numbers and other dialed information for all calls as they are made or received from the device.<br><br>... telephone numbers registered to a particular cell tower for a certain period of time (or [confirmation of] whether a particular telephone number registered on a particular cell tower at a given time). |
| **Automattic** | ... non-public content information (such as private or draft post content, or pending comments). | ... account data such as username, email address, IP address, legal name, physical address, and payment records.<br><br>Basic account information, such as: Username, Email address, Name, Phone number<br><br>Transaction and/or billing information<br><br>Site creation, posting, and revision history information, such as: The date and time (UTC) at which a site was created, The IP address from which a site was created, IP address and user-agent for a post or revision<br><br>Information on commenters on WordPress.com sites.<br><br>... first and last names, phone number, email address currently assigned to a site owner, the date / time stamped IP address from which a site was created, the physical address, and the PayPal transaction information ... |
| **Cheezburger** | ... content information, which includes private messages, images, links, and posts/ comments that have been deleted or otherwise hidden from public view. | |
| **Cisco** | Customer Data is all data (including text, audio, video or image files) that is provided to Cisco in connection with your use of our products or services. Customer Data does not include Administrative Data, Payment Data, Support Data or Telemetry Data ... | Administrative Data is information about customer representatives provided during sign-up, purchase or contracting, or management of products or services. This may include name, address, phone number, IP address and email address, whether collected at the time of the initial agreement or later during management of the products or services. |

*--- Continued on next page ---*

| COMPANY | CONTENT | NON-CONTENT |
|---|---|---|
| **Cisco**(Cont'd) | | Payment Data is the information that you provide when making a purchase or entering into a licensing agreement for products or services. This may include name, billing address, payment instrument number, the security code associated with your payment instrument and other financial data.<br><br>Support Data is the information we collect when you submit a request for support services or other troubleshooting, it may include information about hardware, software, and other details related to the support incident, Examples of details include authentication information, information about the condition of the product, system and registry data about software installations and hardware configurations, and error-tracking files.<br><br>Support Data does not include log, configuration or firmware files, or core dumps, taken from a product and provided to us to help us troubleshoot an issue in connection with a support request.<br><br>Telemetry Data is samples of email, web and network traffic, including but not limited to data on email message and web request attributes and information on how different types of email messages and web requests were handled by or routed through Cisco products. Email message metadata and web requests included in Telemetry Data are anonymized or otherwise obfuscated to remove any personally identifiable information prior to disclosure to any unrelated third party. |
| **CloudFlare** | CloudFlare ... does not have customer content in the traditional sense.<br><br>... content such as abuse complaints or support communications ... | ... customer or billing information ...<br><br>...non-content information, including IP address information. |
| **Comcast** | Content refers to the actual contents of a communication, such as the body of an e-mail or a telephone conversation. | Non-Content refers to information other than the contents of a communication, such as a list of phone numbers or e-mail addresses or header information (signaling, addressing, or routing information).<br><br>... historical information and more detailed information ... |

*--- Continued on next page ---*

| COMPANY | CONTENT | NON-CONTENT |
|---|---|---|
| **Comcast**<br><br>(Cont'd) | | … basic customer account information that is contained in the business records of a service provider.<br><br>… phone numbers and e-mail addresses as they are dialed or sent …<br><br>… incoming phone numbers or e-mail addresses. |
| **CREDO Mobile** | CREDO does not receive or store the content of customer communications sent using our services except customer communications directed to us for customer service purposes. | Customer information refers to non-content information such a customer's name, address, bill information, or handset or account information. |
| **DigitalOcean** | Data that our users generate including copies of Droplets, files on backup, or words in emails to customer support. | "Non-content data" such as basic subscriber information including the information captured at the time of registration such as an alternate email address, name, IP address, login details, billing information, and other transactional information. |
| **DreamHost** | *No definition / examples provided in report.* | |
| **Dropbox** | Content: When we provide "content" information in response to valid legal process, that means we provided the files stored in a person's Dropbox account, in addition to non-content information. | Non-content: When we provide "non-content" information in response to valid legal process, that means we provided subscriber information such as the name and email address associated with the account; the date of account creation and other transactional information like IP addresses. "Non-content" information does not include the files that people store in their Dropbox accounts. |
| **Evernote** | *No definition / examples provided in report.* | |
| **Facebook** | | Non-content data information may include person's name, location and IP history.<br><br>real-time information<br><br>… basic subscriber information, such as name and length of service.<br><br>… IP address logs … |

| COMPANY | CONTENT | NON-CONTENT |
|---|---|---|
| **GitHub** | *No definition / examples provided in report.* | |
| **Google** | … user's search query information and private content stored in a Google Account, such as Gmail messages, documents, photos and YouTube videos.<br><br>*[Gmail]* Email content<br><br>*[YouTube]* Copy of a private video and associated video information; Private message content<br><br>*[Google Voice]* Stored text message content; Stored voicemail content<br><br>*[Blogger]* Private blog post and comment content | … name that you listed when creating the account, and the IP addresses from which you created the account and signed in and signed out (with dates and times).<br><br>… more detailed information about the use of the account. 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.<br><br>… could include the numbers you dial on your phone to reach someone or an IP address issued by an ISP to a subscriber.<br><br>*[Gmail]* Subscriber registration information (e.g., name, account creation information, associated email addresses, phone number); Sign-in IP addresses and associated time stamps; Non-content information (such as non-content email header information); Information obtainable with a subpoena<br><br>*[YouTube]* Subscriber registration information; Sign-in IP addresses and associated time stamps; Video upload IP address and associated time stamp<br><br>*[Google Voice]* Subscriber registration information; Sign-up IP address and associated time stamp; Telephone connection records; Billing information; Forwarding number; Information obtainable with a subpoena<br><br>*[Blogger]* IP address and associated time stamp related to a specified blog post; IP address and associated time stamp related to a specified post comment |
| **Inflection** | *No definition / examples provided in report.* | |
| **Internet Archive** | *No definition / examples provided in report.* | |
| **Kickstarter** | *No definition / examples provided in report.* | |

| COMPANY | CONTENT | NON-CONTENT |
|---|---|---|
| **LinkedIn** | *No definition / examples provided in report.* | |
| **Lookout** | *No definition / examples provided in report.* | |
| **Mapbox** | *No definition / examples provided in report.* | |
| **Medium** | *No definition / examples provided in report.* | |
| **Microsoft** | ... content could include the subject or body of an email, photos stored in OneDrive, address book information, and calendars | Non-content information could include the user's name, billing address, IP history, etc. |
| **Nest** | *-No definition / examples provided in report.* | |
| **Pinterest** | *No definition / examples provided in report.* | |
| **Reddit** | ... content information, which includes private messages and posts/comments that have been deleted or otherwise hidden from public view. | ... subscriber information, which includes IP addresses, the date that an account was created and e- mail addresses. |
| **Silent Circle** | *No definition / examples provided in report.* | |
| **Slack** | *No definition / examples provided in report.* | |
| **Snapchat** | *No definition / examples provided in report.* | |
| **Sonic** | *No definition / examples provided in report.* | |

| COMPANY | CONTENT | NON-CONTENT |
|---|---|---|
| **SpiderOak** | *No definition / examples provided in report.* | |
| **Sprint** | … content (email, text messages, voicemail or pictures) …<br><br>… content of telephone or Internet communications of a Sprint customer for a limited period of time.<br><br>… content of communications, such as text messages and voicemail messages. Sprint currently does not store customer text messages, email or pictures sent or received.<br><br>… location information for a device in real time. | … telephone numbers for all calls that used a specific cell tower to connect to Sprint's network during a specific period of time<br><br>… incoming and outgoing telephone numbers and the locations of the cell towers used during a phone call or when sending or receiving a text message … |
| **T-Mobile** | Real Time Content (e.g., text messages)<br><br>Stored Content (e.g., saved voicemail message)<br><br>Real Time Audio (e.g., phone conversation)<br><br>Real Time Location (e.g., approximate location of a phone/ mobile device)<br><br>Historical Cell Site Location Information (e.g., location of towers that a phone/mobile device used in the past over a specific period of time) | Subscriber Information (e.g., information a customer provides when signing up for service, such as name and address, and call detail information)<br><br>Historical Call Detail Information (e.g., information about calls made in the past, such as start time, duration, numbers called)<br><br>Real Time Call Detail Information (e.g., information on incoming and outgoing phone numbers for a specific phone/ mobile device)<br><br>Historical Cell Tower Dump Information (e.g., list of phone numbers which used a specific tower during a specific period of time) |
| **Time Warner Cable** | | … account identifying information such as name, address, telephone number and IP address. |

| COMPANY | CONTENT | NON-CONTENT |
|---|---|---|
| **Tumblr** | "Blog content" refers to the media and caption of public or private posts, and any messages like Fan Mail. | Account data includes registration email address, how long a Tumblr account has been registered, and login IP addresses. Account data does not include posts made to a blog, whether public or private. |
| **Twitter** | ... contents of communications (e.g., Tweets, DMs). | ... basic subscriber information, such as the email address associated with an account and IP logs.<br><br>... IP address records ... |
| **Verizon** | "Stored content" refers to communications or other data that our users create and store through our services, such as text messages, email or photographs.<br><br>... voice communications ... | ... customer name, address, telephone or other subscriber number, length of service, calling records and payment records.<br><br>... dialing, routing, addressing or signaling information.<br><br>... real-time access to the numbers that a customer dials (or IP addresses that a customer visits) [and] to the numbers that call a customer.<br><br>Non-content refers to records we create such as subscriber information that a customer provides at the time she signs-up for our services, and transactional information regarding the customer's use of our services, such as phone numbers that a customer called.<br><br>... call detail records or similar "transactional" information about communications carried on Verizon's networks. |
| **Wickr** | *No definition / examples provided in report.* | |
| **Wikimedia Foundation** | *No definition / examples provided in report.* | |
| **Yahoo** | Content: Data that our users create, communicate, and store on or through our services. This could include words in a communication (e.g., Mail or Messenger), photos on Flickr, files uploaded, Yahoo Address Book entries, Yahoo Calendar event details, thoughts recorded in Yahoo Notepad or comments or posts on Yahoo Answers or any other Yahoo property. | NCD: Non-content data such as basic subscriber information including the information captured at the time of registration such as an alternate e-mail address, name, location, and IP address, login details, billing information, and other transactional information (e.g., "to," "from," and "date" fields from email headers). |

# MEMO 6: REPORTING ON OUTCOMES & COMPLIANCE WITH REQUESTS

# BEST PRACTICES

## FOR REPORTING ON OUTCOMES & COMPLIANCE WITH REQUESTS

There are a variety of practices for reporting on how a company complies with or responds to requests for user data. One challenge to reporting this information is the difficulty companies face when quantifying their responses to certain requests, such as when a request is challenged but then results in subsequent disclosure, be it partial or full. Given the complexities of compliance and challenging requests, clear and granular reporting on this content is all the more important. *DigitalOcean*'s report demonstrates the current best practices of such reporting. **The best practice — granular reporting — first entails reporting compliance with requests for each different kind of process** (e.g., warrant, subpoena), **and second, reporting on the different ways a company may respond to a request** (e.g., rejected, disclosed content). Reports from Adobe, Apple, CloudFlare, Facebook, Microsoft, and Yahoo demonstrate "Approaching Best Practices," identified on the following page. Approaching Best Practices recognize reporting that falls just short of the best practices standard(s) but is nonetheless deserving of recognition for a demonstrated commitment to informative and comprehensive transparency reporting.




*DigitalOcean* has some of the most granular reporting for responses. DigitalOcean reports five different responses (request still in process, no data found, rejected/no information provided, only NCD disclosed, and content disclosed), for five different legal processes (subpoenas, ECPA court orders, search warrants, wiretap or PRTTs (pen register/trap and trace), and imminent harm requests).

# OTHER PRACTICES OF NOTE

FOR REPORTING ON OUTCOMES & COMPLIANCE WITH REQUESTS

## APPROACHING BEST PRACTICES

"Approaching Best Practices" are strong reporting practices, but ones that could benefit from additional information or granularity. Companies with these practices have demonstrated a clear commitment to informative and comprehensive reporting on outcomes and compliance with requests, but fell just short of inclusion in "Best Practices."

*Adobe* reports four granular responses (account doesn't exist vs. customer registration or transactional information disclosed vs. customer content disclosed vs. request rejected/no information provided) for all processes in aggregate.

*Apple* reports four granular responses (account requests for which data was disclosed vs. when Apple objected vs. when no data was disclosed vs. when non-content was disclosed vs. when some content was disclosed) for all processes in aggregate.

*CloudFlare* reports granularly by process, including outcomes for subpoenas, court orders, search warrants, pen register/trap and trace (PRTT) orders, and wiretap orders. However, CloudFlare only reports whether these requests were "answered" or "in process."

*Facebook* reports granularly by process, including outcomes for search warrants, subpoenas, emergency disclosures, 2703(d) orders, court orders (other), pen registers/trap and traces, and Title III. However, Facebook only reports whether "some data" was produced.

*Microsoft* reports four granular responses (disclosed content vs. only subscriber / transactional data vs. no data found vs. rejected) for all processes in aggregate.

*Yahoo* reports four granular responses (content disclosed vs. no data found vs. rejected vs. only NCD disclosed) for all processes in aggregate.

# CURRENT PRACTICES

## FOR REPORTING ON OUTCOMES & COMPLIANCE WITH REQUESTS

Some companies choose not to report on how they responded to requests for user / customer information or whether they complied with the request at all. Other companies report that information with impressive detail. And yet other companies fall somewhere in the middle. The following chart surveys how U.S. Internet and telecommunications companies report on their responses to, and compliance with, requests for user information.

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Adobe** | Number of **Requests** | **Account Doesn't Exist** | |
| | Number of **Users Impacted** | | |
| | Number of **Requests** | **Customer Registration or Transactional Information Disclosed** | |
| | Number of **Users Impacted** | | |
| | Number of **Requests** | **Customer Content Disclosed** | |
| | Number of **Users Impacted** | | |
| | Number of **Requests** | **Request Rejected/ No Information Provided** | |

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Amazon** | **Subpoenas** | **Full Response** *(#)* | Full response means that Amazon responded to valid legal process by providing all of the information requested. |
| | **Search Warrants** | | |
| | **Other Court Orders** | | |
| | **Subpoenas** | **Partial Response** *(#)* | Partial response means that Amazon responded to valid legal process by providing only some of the information requested. |
| | **Search Warrants** | | |
| | **Other Court Orders** | | |
| | **Subpoenas** | **No Response** *(#)* | No response means that Amazon responded to valid legal process by providing none of the information requested. |
| | **Search Warrants** | | |
| | **Other Court Orders** | | |
| **AOL** | *Report does not disclose data on responses to / compliance with requests.* | | |
| **Apple** | Number of **Device Requests** | Where **Some Data Was Provided** | The number of law enforcement requests that resulted in Apple providing relevant device information, such as registration, subscriber, service, repair, and purchase information in response to valid legal process. |
| | Percentage of **Device Requests** | Where **Some Data Was Provided** | The percentage of law enforcement requests that resulted in Apple providing some relevant device information in response to valid legal process. |

*--- Continued on next page ---*

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Apple** (Cont'd) | Number of **Account Requests** | Where **No Data Was Disclosed** | The number of law enforcement requests that resulted in Apple providing no customer information whatsoever. |
| | Number of **Account Requests** | Where **Apple Objected** | The number of law enforcement requests that resulted in Apple refusing to provide some data based on various grounds, such as jurisdiction, improper process, insufficient process, invalid process, or where the scope of the request was excessively broad. For example, Apple may object to a law enforcement request as "invalid" if it were not signed. |
| | Number of **Account Requests** | Where **NonContent Data Was Disclosed** | The number of law enforcement requests that resulted in Apple providing only subscriber or transactional information, but not content. For example, Apple may provide subscriber information and a limited purchase history in response to valid legal process. |
| | Number of **Account Requests** | Where **Some Content Was Disclosed** | The number of law enforcement requests where Apple determined that an account request was lawful and provided content such as iCloud email, contacts, calendar, or Photo Stream content. Apple only provides user account content in extremely limited circumstances. |
| | Percentage of **Account Requests** | Where **Some Data Was Disclosed** | The percentage of law enforcement requests that resulted in Apple providing some iCloud, iTunes, or Game Center data. |
| | Number of **Accounts** | For Which **Data Was Disclosed** | The number of discernible accounts, based on specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers, for which Apple provided some iCloud, iTunes, or Game Center data. |

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **AT&T** | **Demands** | **Rejected/ Challenged** *(#) (#)* | We ensure that we receive the appropriate type of demand for the information requested. In this category, we include the number of times we rejected a demand or provided only partial information or no information in response to a demand. |
| | **Demands** | **Partial or No Information** *(#)* | Here are a few reasons why certain demands fall into this category:<br>• The wrong type of demand is submitted by law enforcement. For instance, we will reject a subpoena requesting a wiretap, because either a probable cause court order or search warrant is required.<br>• The demand has errors, such as missing pages or signatures.<br>• The demand was not correctly addressed to AT&T.<br>• The demand did not contain all of the elements necessary for a response.<br>• We had no information that matched the customer or equipment information provided in the demand. |
| **Automattic** | Percentage of **requests** | where **some or all information was produced** | |
| **Cheezburger** | **Total** | **Complied** *(#)* | |
| **Cisco** | *Report does not disclose data on responses to / compliance with requests.* | | |

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **CloudFlare** | **Subpoenas** | **answered** *(#)* | The data presented below covers the period from July 1, 2014 to December 31, 2014. So, for example, a request received in June 2014, but not processed until July 2014 will show as both "Requests received" and "Requests in process."<br><br>Also, requests for which we are waiting for a response from law enforcement before moving forward may also be reflected in "Requests in process." |
| | **Court orders** | | |
| | **Search warrants** | | |
| | **Pen register/Trap and trace (PRTT) orders** | | |
| | **Wiretap orders** | | |
| | **Subpoenas** | **in process** *(#)* | |
| | **Court orders** | | |
| | **Search warrants** | | |
| | **Pen register/Trap and trace (PRTT) orders** | | |
| | **Wiretap orders** | | |
| **Comcast** | *Report does not disclose data on responses to / compliance with requests.* | | |
| **CREDO Mobile** | Number of **governmental requests** | for which **some or all information requested was produced** | Includes requests for which CREDO had no responsive information. |

*--- Continued on next page ---*

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **CREDO Mobile**<br><br>(Cont'd) | Number of **governmental requests** | for which **customer communication content information requested (including wiretap requests) was produced** | |
| | Number of **customer accounts** | for which **customer information was produced** | |
| **DigitalOcean** | **Subpoenas** | **Request still in process** *(#)* | Request has been received by DigitalOcean but is awaiting further processing or for a response from law enforcement. |
| | **ECPA Court Order** | | |
| | **Search Warrant** | | |
| | **Wiretap or PRTT** | | |
| | **Imminent Harm** | | |

*--- Continued on next page ---*

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| | **Subpoenas** | **No Data Found** *(#)* | The user account information either doesn't exist or has been deleted. |
| | **ECPA Court Order** | | |
| | **Search Warrant** | | |
| | **Wiretap or PRTT** | | |
| | **Imminent Harm** | | |
| **DigitalOcean** [Cont'd] | **Subpoenas** | **Rejected / No Information Provided** *(#)* | 1) The request was duplicative of a request we already responded to<br>2) DO objected to the request<br>3) Law enforcement withdrew the request<br>4) The request failed to include enough information<br>5) The request expired |
| | **ECPA Court Order** | | |
| | **Search Warrant** | | |
| | **Wiretap or PRTT** | | |
| | **Imminent Harm** | | |
| | **Subpoenas** | **Only NCD disclosed** *(#)* | "Non-content data" such as basic subscriber information including the information captured at the time of registration such as an alternate email address, name, IP address, login details, billing information, and other transactional information. |
| | **ECPA Court Order** | | |
| | **Search Warrant** | | |

*--- Continued on next page ---*

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **DigitalOcean**<br><br>[Cont'd] | **Wiretap or PRTT** | **Only NCD disclosed** *[#]*<br><br>[Cont'd] | |
| | **Imminent Harm** | | |
| | **Subpoenas** | **Content Disclosed** *[#]* | Data that our users generate including copies of Droplets, files on backup, or words in emails to customer support. |
| | **ECPA Court Order** | | |
| | **Search Warrant** | | |
| | **Wiretap or PRTT** | | |
| | **Imminent Harm** | | |
| **DreamHost** | Percentage of **requests** | **complied** | ... the percentage of requests we complied with where partial data was produced. |
| **Dropbox** | To **each warrant** | **Does not exist** *[#]* | Account did not exist: This means that law enforcement specified an account in their request, but that account did not exist. |
| | To **each account listed *(in warrants)*** | | |
| | To **each subpoena** | **Does not exist** *[#]* | |
| | To **each account listed *(in subpoenas)*** | | |
| | **Court orders** | **Account(s) did not exist** *[#]* | |

*--- Continued on next page ---*

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Dropbox** [Cont'd] | To **each subpoena** | **Content produced** *(#)* | When we provide "content" information in response to valid legal process, that means we provided the files stored in a person's Dropbox account, in addition to non-content information. |
| | To **each account listed *(in subpoenas)*** | | |
| | **Court orders** | **Content provided** *(#)* | |
| | To **each warrant** | **Content and non-content produced** *(#)* | |
| | To **each account listed *(in warrants)*** | | |
| | To **each subpoena** | **Non-content produced** *(#)* | When we provide "non-content" information in response to valid legal process, that means we provided subscriber information such as the name and email address associated with the account; the date of account creation and other transactional information like IP addresses. "Non-content" information does not include the files that people store in their Dropbox accounts. |
| | To **each account listed *(in subpoenas)*** | | |
| | **Court orders** | **Non-content provided** *(#)* | |
| | To **each warrant** | **No information provided** *(#)* | This means that we didn't provide any information in response to the request for one or more of the following reasons: (1) the request was duplicative of a request that we already responded to; (2) Dropbox objected to the request; (3) law enforcement withdrew the request; or (4) the request failed to specify an account. |
| | To **each account listed *(in warrants)*** | | |
| | To **each subpoena** | | |
| | To **each account listed *(in subpoenas)*** | | |
| | **Court orders** | | |

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Evernote** | **Criminal requests** from US governmental entities | **Responded with Data** *(#)* | ... the number of requests to which we responded by disclosing user data. |
| **Facebook** | Total **Requests** | where **some data produced** *(%)* | |
| | **Search Warrant** | | |
| | **Subpoena** | | |
| | **Emergency Disclosures** | | |
| | **Court Order [18 USC § 2703(d)]** | | |
| | **Court Order [Other]** | | |
| | **Pen Register/Trap and Trace** | | |
| | **Title III** | | |
| **GitHub** | Percentage of **Requests** | Where **Information was Disclosed** | There are several reasons why information may not be disclosed in response to a legal request. It may be that we do not have the requested data. It may be that the request was too vague such that we could not identify the data, or that it was otherwise defective. Sometimes the requesting party may simply withdraw the request. Other times, the requesting party may revise and submit another one. In cases where one request was replaced with a second, revised request, we would count that as two separate requests received. However, if we responded only to the revision, we would count that only as having responded to one request. |
| | Percentage of **Requests** | **Nothing Disclosed** | |
| | Percentage of **Requests** | **Some or All Requested Information Disclosed** | |

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Google** | Percentage of **Requests** | **Where Some Data Produced** | We report percentages for criminal requests from July 2010 onward. Those percentages reflect the number of requests we responded to by producing some information. |
| **Inflection** | **US Govt. Subpoenas** | **Produced some info** *(#)* | |
| | **US Civil Subpoenas** | | |
| | **US Search Warrants** | | |
| | **Emergency requests** | | |
| | % of **all demands** | **produced at least some customer information** | |
| **Internet Archive** | User **accounts** | for which **data was handed over** *(#)* | |
| **Kickstarter** | **Subpoenas** | we **released some information in response** *(#)* | Of the 8 requests, 3 were in the form of subpoenas, and we released some information in response. We did not produce any information in response to the other 5 requests. |
| | **Other requests** | we **did not produce any information** *(#)* | |
| **LinkedIn** | Percentage of **Requests** | to which **LI Provided Some Data** | |
| **Lookout** | *[for all processes, in aggregate]* | **Disclosure Rate** *(%)* | |
| **Mapbox** | *Report does not disclose data on responses to / compliance with requests.* | | |

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Medium** | *Report does not disclose data on responses to / compliance with requests.* | | |
| **Microsoft** | *[for all processes, in aggregate]* | % **Disclosed Content** | The number of court orders found to be lawful, and therefore at least some customer content was disclosed. Such content could include the subject or body of an email, photos stored in OneDrive, address book information, and calendars. In most cases, a court order that requires the disclosure of customer content will also require the disclosure of non-content data (see definition below). |
| | *[for all processes, in aggregate]* | % **Only Subscriber / Transactional Data** | The number of law enforcement requests determined to be lawful, and therefore only non-content information was disclosed. Non-content information could include the user's name, billing address, IP history, etc. |
| | *[for all processes, in aggregate]* | % **No Data Found** | The number of law enforcement requests and/or court orders where our Compliance Team found no data in our systems related to the request and/or order, and therefore disclosed no customer information to law enforcement. |
| | *[for all processes, in aggregate]* | % **Rejected** | The number of law enforcement requests and/or court orders rejected because we determined they failed to satisfy the relevant legal requirements, or where we successfully redirected law enforcement to obtain the information directly from the customer. As a result, no customer data of any kind was disclosed. |
| **Nest** | *Report does not disclose data on responses to / compliance with requests.* | | |
| **Pinterest** | **Federal** | **Compliance w/ partial or full production** *[%]* | |

*--- Continued on next page ---*

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Pinterest** [Cont'd] | **State/Local** | **Compliance w/ partial or full production** *[%]* | |
| | **Civil Requests** | **Compliance w/ partial or full production** *[%]* | |
| **Reddit** | # of **requests** | where **some info was disclosed** | |
| | % of **requests** | where **some user info was disclosed** | |
| **Silent Circle** | Number of **Users' Data/Metadata** | **Surrendered** | |
| **Slack** | *Report does not disclose data on responses to / compliance with requests.* | | |
| **Snapchat** | Percentage of **requests** | where **some data was produced** | |
| **Sonic** | Total Number of **Data** | **Surrendered** | |
| **SpiderOak** | Number of **User's Data** | **Surrendered** | |
| | Rate of **User's Data** | **Surrendered** | |
| **Sprint** | *Report does not disclose data on responses to / compliance with requests.* | | |
| **T-Mobile** | *Report does not disclose data on responses to / compliance with requests.* | | |

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Time Warner Cable** | *[for all processes, in aggregate]* | **No Data Disclosed** *[%]* | |
| | *[for all processes, in aggregate]* | **Only Subscriber Information** *[%]* | |
| | *[for all processes, in aggregate]* | **Disclosed Content** *[%]* | |
| **Tumblr** | % **Account Data** | **Produced** | |
| | % **Blog Content** | **Produced** | |
| | *[for all processes, in aggregate]* | **Something Produced** *[%]* | |
| | *[for all processes, in aggregate]* | **Nothing Produced** *[%]* | In cases where no content or data was produced, the requests may have been withdrawn, or were defective, or we may have objected to the requests on legal grounds. |
| **Twitter** | *[for all processes, in aggregate]* | percentage where **some information produced** | We may not comply with requests for a variety of reasons. For example:<br>• We do not comply with requests that fail to identify a Twitter account.<br>• We may seek to narrow requests that are overly broad.<br>• In other cases, users may have challenged the requests after we've notified them. |
| **Verizon** | % of **demands** we received | **rejected as invalid** | We might reject a demand as legally invalid for a number of reasons, including that a different type of legal process is needed for the type of information requested. When we reject a demand as invalid, we do not produce any information. |

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Wickr** | *Report does not disclose data on responses to / compliance with requests.* | | |
| **Wikimedia Foundation** | *[for all processes, in aggregate]* | **Information Produced** *(#)* | When we say 'information produced', we mean that as a result of a legal process (such as a subpoena) that was legally valid, some or all of the nonpublic user information requested by that legal process was produced by WMF to the requesting party.'Information produced' also applies to rare situations where we voluntarily disclose personal information to voluntarily disclose personal information to law enforcement, usually in order to prevent imminent bodily harm or death. |
| | **Criminal Subpoenas** | **Information Produced** *(#)* | |
| | **Informal Government Requests** | **Information Produced** *(#)* | |
| | **Court Orders** | **Information Produced** *(#)* | |
| **Yahoo** | *[for all processes, in aggregate]* | **Rejected** *(#)* | Rejected: 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. We carefully review Government Data Requests for legal sufficiency and interpret them narrowly in an effort to produce the least amount of data necessary to comply with the request. |
| | *[for all processes, in aggregate]* | **Rejected** *(%)* | |
| | *[for all processes, in aggregate]* | **No Data Found** *(#)* | No Data Found: Yahoo produced no data in response to the Government Data Request because no responsive data could be found (i.e., the account didn't exist or there was no data for the date range specified by the request). |
| | *[for all processes, in aggregate]* | **No Data Found***(%)* | |

*--- Continued on next page ---*

| COMPANY | PROCESS / REQUEST TYPE | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF TERMS |
|---|---|---|---|
| **Yahoo**<br><br>(Cont'd) | *[for all processes, in aggregate]* | **Only NCD Disclosed** *(#)* | |
| | *[for all processes, in aggregate]* | **Only NCD Disclosed** *(%)* | |
| | *[for all processes, in aggregate]* | **Content Disclosed** *(#)* | |
| | *[for all processes, in aggregate]* | **Content Disclosed** *(%)* | |
| | **Global Emergency Disclosure Requests** | Percentage of **Requests Resulting in Disclosure of Data** | In addition to Government Data Requests, Yahoo receives requests from governments seeking information in emergency situations, i.e. the disclosure of information is sought to save a life or prevent serious physical harm. The chart below represents the number of such requests that Yahoo received globally during the reporting period, the number of accounts specified in those requests, and the percentage of the requests that resulted in the disclosure of some information. |

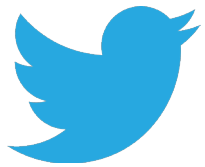
# MEMO 7: REPORTING ON USER NOTIFICATION

# BEST PRACTICES

## FOR REPORTING ON USER NOTIFICATION

*Twitter*'s report demonstrates the **best practice of clear, comprehensive, and granular reporting on notification of users specified in legal process requests.** Reports from Dropbox and GitHub demonstrate "Approaching Best Practices," identified on the following page. Approaching Best Practices recognize reporting that falls just short of the best practices standard(s) but is nonetheless deserving of recognition for a demonstrated commitment to informative and comprehensive transparency reporting. Additionally Tumblr's report demonstrates "Notable Practices," also identified on the following page. Notable Practices are innovative, unique, or noteworthy practices, but ones that may not be feasible for all companies.

Few companies engage in the practice of reporting on whether they provided user notice upon receiving or responding to requests for user information. Within the companies that do report on user notification, there are a wide variety of approaches to reporting that information and on the specifics of their user notification policies, including whether their policy is to notify prior to, concurrently with, or after disclosure. Despite how few companies disclose user notification statistics, and how each has taken a different approach, reporting on user notification can be fairly straightforward: **The best practice is to report on three types of notifications: 1) When a request was under seal and the user could not be notified, 2) When a request was not under seal and the user was notified, and 3) When a request was not under seal and the user was not notified.**



*Twitter*'s practice of reporting on all three categories of user notice – whether a request was under seal (and therefore Twitter was legally prohibited from notifying users), whether user notice was provided (and request was not under seal), and whether user notice was not provided (and request was not under seal) – offers the most transparent and complete view of a company's approach to informing users that they have been the subject of a request.

# OTHER PRACTICES OF NOTE

FOR REPORTING ON USER NOTIFICATION

## APPROACHING BEST PRACTICES

"Approaching Best Practices" are strong reporting practices, but ones that could benefit from additional information or granularity. Companies with these practices have demonstrated a clear commitment to informative and comprehensive reporting on user notification, but fell just short of inclusion in "Best Practices."




*Dropbox* has granular reporting of user notification on a process-by-process basis, but reports only whether notice was provided. Dropbox reports on whether notice was provided in response to each search warrant, each account listed in search warrants, to each subpoena, to each account listed in subpoenas, and to court orders.




*GitHub* reports two user notification statistics: the percentage of disclosures where the company notified affected users and those times when it was prohibited from notifying users. GitHub's reporting easily stands out in a field with so few companies reporting any data on user notification.

## NOTABLE PRACTICES

"Notable practices" are innovative approaches to reporting. Notable practices may not be feasible for all companies, but for those with the resources and opportunity, they offer a chance to add additional transparency and information.



*Tumblr* has taken a notable and novel approach to reporting on user notification. The company reports the percentage of all requests accompanied by a non-disclosure order, but also reports on two categories of notification — the percentages of users notified and the percentages of users not notified — for eight different categories of investigation, such as "bullying/harassment," "harm to minors," and "invasion of privacy" investigations.

# CURRENT PRACTICES

## FOR REPORTING ON USER NOTIFICATION

The following table details how companies report on whether and when a user was notified after a company received or responded to a government request for user information (excluding national security requests). Few companies engage in the practice of reporting on user notification.

| COMPANY | VALUE REPORTED | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF DATA REPORTED |
|---|---|---|---|
| **Adobe** | *Report does not disclose data on user notification.* | | |
| **Amazon** | *Report does not disclose data on user notification.* | | |
| **AOL** | *Report does not disclose data on user notification.* | | |
| **Apple** | *Report does not disclose data on user notification.* | | |
| **AT&T** | *Report does not disclose data on user notification.* | | |
| **Automattic** | *Report does not disclose data on user notification.* | | |
| **Cheezburger** | *Report does not disclose data on user notification.* | | |
| **Cisco** | *Report does not disclose data on user notification.* | | |
| **CloudFlare** | *Report does not disclose data on user notification.* | | |
| **Comcast** | *Report does not disclose data on user notification.* | | |

| COMPANY | VALUE REPORTED | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF DATA REPORTED |
|---|---|---|---|
| **CREDO Mobile** | *Report does not disclose data on user notification.* | | |
| **DigitalOcean** | *Report does not disclose data on user notification.* | | |
| **DreamHost** | *Report does not disclose data on user notification.* | | |
| **Dropbox** | To **each warrant** | **Notice provided** *(#)* | Governments continue to request that we not notify users of requests for their data, even when there is no legal basis for the requests. We received 71 such requests between July and December 2014 and responded by informing the requesting agency of our policy to always provide notice unless prohibited by a valid court order (or equivalent). |
| | To **each account listed *(in warrants)*** | | |
| | To **each subpoena** | | |
| | To **each account listed *(in subpoenas)*** | | |
| | **Court orders** | | |
| **Evernote** | *Report does not disclose data on user notification.* | | |
| **Facebook** | *Report does not disclose data on user notification.* | | |
| **GitHub** | Percentage of **Disclosures** | Where **Affected Users Were Provided Notice** | |
| | Percentage of **Disclosures** | **Prohibited from Providing Notice** | |
| **Google** | *Report does not disclose data on user notification.* | | |

| COMPANY | VALUE REPORTED | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF DATA REPORTED |
|---|---|---|---|
| **Inflection** | Government **demands** we received | **requested that we not disclose the existence of the request to the affected customer.** *(#)* | |
| **Internet Archive** | *Report does not disclose data on user notification.* | | |
| **Kickstarter** | *Report does not disclose data on user notification.* | | |
| **LinkedIn** | *Report does not disclose data on user notification.* | | |
| **Lookout** | *Report does not disclose data on user notification.* | | |
| **Mapbox** | *Report does not disclose data on user notification.* | | |
| **Medium** | *Report does not disclose data on user notification.* | | |
| **Microsoft** | *Report does not disclose data on user notification.* | | |
| **Nest** | *Report does not disclose data on user notification.* | | |
| **Pinterest** | *Report does not disclose data on user notification.* | | |
| **Reddit** | # of **requests** | with **legally binding gag orders** | Many government requests we receive contain demands to withhold notice from users that carry no legal weight. We actively disregard these non-binding demands. |
| **Silent Circle** | *Report does not disclose data on user notification.* | | |

| COMPANY | VALUE REPORTED | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF DATA REPORTED |
|---|---|---|---|
| **Slack** | *Report does not disclose data on user notification.* | | |
| **Snapchat** | *Report does not disclose data on user notification.* | | |
| **Sonic** | *Report does not disclose data on user notification.* | | |
| **SpiderOak** | *Report does not disclose data on user notification.* | | |
| **Sprint** | *Report does not disclose data on user notification.* | | |
| **T-Mobile** | *Report does not disclose data on user notification.* | | |
| **Time Warner Cable** | *Report does not disclose data on user notification.* | | |
| **Tumblr** | *[for all processes, in aggregate]* | **Non-Disclosure Order** *[%]* | ... a court legally prohibited us from notifying our users about the request. |
| | *[for all processes, in aggregate]* | **No Non-Disclosure Order** *[%]* | |
| | **Bullying/ Harassment Investigations** | **Notice Provided** *[%]* | ... cases when we complied, at least in part, with requests for user information ...<br><br>... in some cases, we provide user notice after having complied with a government data request. |
| | **Harm to Minors Investigations** | | |
| | **Invasion of Privacy Investigations** | | |

*--- Continued on next page ---*

| COMPANY | VALUE REPORTED | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF DATA REPORTED |
|---|---|---|---|
| | **Invasion of Privacy Investigations** | **Notice Provided** *(%)*<br><br>(Cont'd) | |
| | **National Security and Cybercrime Investigations** | | |
| | **National Suicide Investigations** | | |
| | **Violent Crimes Investigations** | | |
| | **Other Investigations** | | |
| **Tumblr**<br><br>(Cont'd) | **Bullying/ Harassment Investigations** | **No Notice Provided** *(%)* | … if users were not notified prior to account data disclosure, it was for at least one of the following reasons:<br><br>• The request was combined with a binding non-disclosure order;<br><br>• Notice was not practicable due to the threat of death or serious injury; or<br><br>• The case presented a serious threat to public safety. |
| | **Harm to Minors Investigations** | | |
| | **Invasion of Privacy Investigations** | | |
| | **National Security and Cybercrime Investigations** | | |
| | **National Suicide Investigations** | | |
| | **Violent Crimes Investigations** | | |
| | **Other Investigations** | | |

| COMPANY | VALUE REPORTED | RESPONSE REPORTED | ADDITIONAL INFORMATION / EXPLANATION OF DATA REPORTED |
|---|---|---|---|
| **Twitter** | Percentage of **requests** | **under seal** | 'Under seal' means that a court has issued an order legally prohibiting us from notifying affected users (or anyone else) about the request. |
| | Percentage | where **user notice provided** | When not prohibited, we send affected users notice of our receipt of a request for their information, including a copy of the legal process. |
| | Percentage | **not under seal and no notice provided** | Percentage of requests not under seal and no notice provided for one or more of the following reasons:<br>• The request was withdrawn by the requester prior to any disclosure.<br>• No information was disclosed in response to the request.<br>• The request was defective (e.g., improper jurisdiction, no valid Twitter @username), thus no action was taken and no information disclosed.<br>• The request was an exigent emergency disclosure request; see our Guidelines for Law Enforcement for more about emergencies.<br>• Local law may prohibit us from providing notice. |
| **Verizon** | *Report does not disclose data on user notification.* | | |
| **Wickr** | *Report does not disclose data on user notification.* | | |
| **Wlkimedia Foundation** | *Report does not disclose data on user notification.* | | |
| **Yahoo** | *Report does not disclose data on user notification.* | | |

# MEMO 8: REPORTING ON NATIONAL SECURITY ORDERS

# OVERVIEW: REPORTING ON NATIONAL SECURITY ORDERS

National security orders are authorized under the **Foreign Intelligence Surveillance Act (FISA)** and the **Stored Communications Act (SCA)**. There are two types of national security orders:

> 1) Orders authorized by FISA and issued by the specialized **Foreign Intelligence Surveillance Court (FISC)** (50 U.S.C. §1801 et. seq.). The FISC issues court orders authorizing a wide range of surveillance and data collection.
>
> 2) **National Security Letters (NSLs)** (18 U.S.C. §2709) authorized by the SCA. NSLs are secret subpoenas for certain basic subscriber information and non-content transactional data that prosecutors may use to demand information they determine is relevant to an anti-terrorism or espionage investigation.

Reporting on NSLs and FISA orders is more restricted than reporting on other types of government requests for information because these national security orders come with non-disclosure agreements (a.k.a. "gag orders"). Prior to the June 2015 passage of the **USA FREEDOM Act**,[1] companies wanting to report on these orders were subject to unclear and severely restrictive reporting measures.

Before January 2014, companies could not even acknowledge receipt of a national security order. Following a **settlement**[2] with the U.S. Department of Justice, five companies (Facebook, Google, LinkedIn, Microsoft, Yahoo) were permitted to report on national security orders under one of two restrictive structures: **Option 1** allowed reporting on the number of NSLs, FISA orders for content, and FISA orders for non content, each in bands of 1,000. **Option 2** allowed reporting in bands of 500 if all orders were reported in aggregate. There were similar restrictions on reporting on the number of selectors targeted and accounts affected by orders.

While the January 2014 settlement created specific structures for reporting on national security orders, confusion remained, as companies not party to the settlement were unsure whether and how they could report on these orders. At the same time, at least one company, Twitter, has refused to report on national security orders under the terms of the January 2014 settlement. Twitter has sued the DOJ and contends that the restrictions on disclosure are an unconstitutional prior restraint and a violation of the company's First Amendment rights. The DOJ has called for dismissal of the lawsuit. A large and wide-ranging group of Internet and telecommunications companies, including Wikipedia and Automattic, have shown support for Twitter's challenge to the DOJ rules by filing amicus briefs in support of the social media company.

Following the passage of the USA FREEDOM Act, companies now have four options for reporting on national

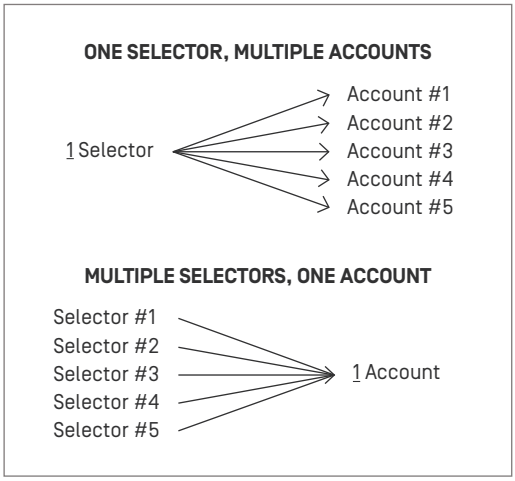
[1] Full text available at https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf
[2] Settlement agreement letter available at http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf

security orders. The new reporting structures remain restrictive but allow for more flexibility than those in the January 2014 DOJ settlement. Under the first two reporting options, companies can share the number of national security letters, FISA orders for content, and the number of FISA orders for non-content with which a company had to comply in bands of either 1000 (**Option 1**) or 500 (**Option 2**). The same bands can be used to report on customer selectors targeted in each of those orders. Under **Option 3**, the company may report on the aggregate number of orders with which it had to comply and also the aggregate number of customer selectors targeted by those orders, each in bands of 250. The data reported under Options 1, 2, and 3 is subject to an 18-month delay and can be reported semiannually. Under **Option 4**, companies can report in bands of 100, however, NSLs and FISC orders must be aggregated, customer selectors targeted by those orders also must be reported in aggregate, and reporting can be on no more than an annual basis.

**Reporting on the Subjects of National Security Orders: January 2014 Settlement vs. USA FREEDOM ACT**

| ORDER | JANUARY 2014 SETTLEMENT | | USA FREEDOM ACT |
|---|---|---|---|
| | OPTION 1 | OPTION 2 | |
| FISC | customer **selectors targeted** | customer **selectors targeted** *(in aggregate)* | customer **selectors targeted** |
| NSLs | customer **accounts affected** | | customer **selectors targeted** |

Another notable change to the reporting structures in the USA FREEDOM Act is how the subjects of requests can be reported. Under Option 1 of the January 2014 DOJ settlement, companies could report on the number of "**customer selectors targeted**" by FISC orders (both content and non-content), but only on the number of "**customer accounts affected**" by NSLs. Under Option 2, companies could report on the combined number of "customer selectors targeted" by NSLs and FISC orders.




Now, under any of the four USA FREEDOM Act reporting structures, companies can report the number of **customer selectors targeted** for both FISC orders and NSLs. Further, the language and legislative history of the Act suggest that additional reporting may be permitted. In a May 2015 report to the Committee on the Judiciary, Chairman Bob Goodlatte explained that the language of the USA FREEDOM Act's reporting provisions 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*." With that intent, companies may also be permitted to report on the number of "**accounts responsive to**" a request. Reporting both the number of customer selectors targeted by national security orders, as well as the number of accounts responsive to/impacted by those orders would bring a welcome amount of granularity and clarity to reporting.

# COMPARING USA FREEDOM ACT REPORTING STRUCTURES

*As outlined in the USA FREEDOM Act of 2015:*

| ORDERS ARE REPORTED ... | OPTION 1 | OPTION 2 | OPTION 3 | OPTION 4 |
|---|---|---|---|---|
| In bands of: | 1,000<br>*Starting with 0-999* | 500<br>*Starting with 0-499* | 250<br>*Starting with 0-249* | 100<br>*Starting with 0-99* |
| No more frequently than: | Semiannually | Semiannually | Semiannually | Annually |
| For a time period covering: | NSLs: Previous 180 Days<br>FISA Orders: 180 Days | | Previous 180 Days | 1 Year |
| With a mandatory reporting delay of: | NSLs: N/A<br>FISA Orders: ≥ 180 Days* | | 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 | ✓ | ✓ | ✓<br>Combined | ✓<br>Combined |
| # of FISA Orders for Non-Content | ✓ | ✓ | | |
| # of Customer Selectors Targeted by National Security Letters | ✓ | ✓ | | |
| # of Customer Selectors Targeted by FISA Orders for Content | ✓ | ✓ | ✓<br>Combined | ✓<br>Combined |
| # of Customer Selectors Targeted by FISA Orders for Non-Content | ✓^ | ✓ | | |

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

*^ Customer selectors targeted under Title IV, Title V § 501(b)(2)(B), and Title V § 501(b)(2)(C) are reported separately (i.e., each in its own band of 1,000)*

# CURRENT PRACTICES

## FOR REPORTING ON NATIONAL SECURITY ORDERS (UNDER JANUARY 2014 DOJ SETTLEMENT)

Because The Transparency Reporting Toolkit *Survey & Best Practice Memos* cover reporting practices prior to July 10, 2015 and the USA FREEDOM Act was not passed until June 2, the following table covers pre-USA FREEDOM Act reporting practices. Prior to passage of the USA FREEDOM Act, many companies reported on national security orders under the terms of the January 2014 DOJ settlement. Even companies not party to the settlement modeled their reporting on the terms put forth by the Deputy Attorney General, which permitted reporting in bands of 250 (with NSLs and FISA orders aggregated) or bands of 1000 (with NSLs and FISA orders separated). However, there are variations in reporting. While the DOJ settlement outlined two explicit reporting structures, many companies used modified versions of those structures.

| COMPANY | DOJ OPTION 1<br>Separate bands of 0-999 | DOJ OPTION 2<br>Aggregated bands of 0-249 | OTHER REPORTING METHODS & ADDITIONAL INFORMATION REPORTED |
|---|---|---|---|
| **Adobe** | | | X<br>No National Security Requests Received<br>As of the end of FY 2014, Adobe still has not received any form of national security process, such as a National Security Letter (NSL) or Foreign Intelligence Surveillance Act (FISA) order. |
| **Amazon** | | X | |
| **AOL** | X | | |
| **Apple** | | X | X<br>To date, Apple has not received any orders for bulk data. |
| **AT&T** | X | | |

| COMPANY | DOJ OPTION 1<br>Separate bands of 0-999 | DOJ OPTION 2<br>Aggregated bands of 0-249 | OTHER REPORTING METHODS & ADDITIONAL INFORMATION REPORTED |
|---|---|---|---|
| **Automattic** | | X<br>*(for July 1 - Dec 31, 2013)* | X<br>National Security Requests Received: None.<br>User Accounts Affected: None.<br>We are pleased to report that we received no National Security Requests during 2014 or so far in 2015<br>*(for Jan 1 - Dec 31, 2015)* |
| **Cheezburger** | | | X<br>Warrant Canary Statement: As of February 5, 2015, Cheezburger has never received a National Security Letter, an order under the Foreign Intelligence Surveillance Act, or any other classified request for user information. |
| **Cisco** | | | X<br>U.S. national security agencies*: 0<br>*Includes Foreign Intelligence Surveillance Act (FISA) court orders, warrants and directives, and FBI National Security Letters. |
| **CloudFlare** | | X | |
| **Comcast** | X | | |
| **CREDO Mobile** | X | | |
| **DigitalOcean** | | X | |
| **DreamHost** | X | | |

| COMPANY | DOJ OPTION 1<br>Separate bands of 0-999 | DOJ OPTION 2<br>Aggregated bands of 0-249 | OTHER REPORTING METHODS & ADDITIONAL INFORMATION REPORTED |
|---|---|---|---|
| **Dropbox** | | X | |
| **Evernote** | | | X<br>0-250 |
| **Facebook** | X | | |
| **GitHub** | | X | |
| **Google** | X | | |
| **Inflection** | | | X<br>As of March 31, 2015, Inflection has never received a classified request pursuant to the national security laws of the United States or any other country. In other words, Inflection has not received a National Security Letter or a request under the Foreign Intelligence Surveillance Act. |
| **Internet Archive** | | | X<br>National Security Requests: 0<br>FISA Requests: 0 |
| **Kickstarter** | | | X<br>To date, Kickstarter has not received any national security requests for user information. |
| **LinkedIn** | | X | |

| COMPANY | DOJ OPTION 1<br>Separate bands of 0-999 | DOJ OPTION 2<br>Aggregated bands of 0-249 | OTHER REPORTING METHODS & ADDITIONAL INFORMATION REPORTED |
|---|---|---|---|
| **Lookout** | | | **X**<br><br>... as of the date of this report, Lookout has not received a national security order and we have not been required by a FISA court to keep any secrets that are not in this transparency report. |
| **Mapbox** | *Report does not (specifically) disclose national security orders received. Has not received any government requests for information.* | | |
| **Medium** | | | **X**<br><br>National Security Letters: 0<br>Orders issued by the Foreign Intelligence Surveillance Court: 0<br><br>We are pleased to report that we have received zero national security demands to date. |
| **Microsoft** | **X** | | |
| **Nest** | | | **X**<br><br>Overall, we've seen fewer than 25 requests, and never any National Security Letters or orders for user content or non-content information under the Foreign Intelligence Surveillance Act (FISA). |
| **Pinterest** | | | **X**<br><br>National security: 0 |
| **Reddit** | | | **X**<br><br>As of January 29, 2015, reddit has never received a National Security Letter, an order under the Foreign Intelligence Surveillance Act, or any other classified request for user information. |

| COMPANY | DOJ OPTION 1<br>Separate bands of 0-999 | DOJ OPTION 2<br>Aggregated bands of 0-249 | OTHER REPORTING METHODS & ADDITIONAL INFORMATION REPORTED |
|---|---|---|---|
| **Silent Circle** | *Report does not (specifically) disclose national security orders received. Has not received any government requests for information.* | | |
| **Slack** | *Report does not (specifically) disclose national security orders received. Has not received any government requests for information.* | | |
| **Snapchat** | | | **X**<br>FISA: Data subject to six month reporting delay<br>NSL Requests: 0<br>Account Identifiers: N/A<br>Percentage of requests where some data was produced: N/A |
| **Sonic** | **X** | | |
| **SpiderOak** | *Report does not (specifically) disclose national security orders received.* | | |
| **Sprint** | **X** | | |
| **T-Mobile** | **X** | | |
| **Time Warner Cable** | | **X** | |
| **Tumblr** | | | **X**<br>As of the date of publication, we have never received a National Security Letter, FISA order, or other classified request for user information. |
| **Twitter** | *Report does not disclose national security orders received. In October 2014 Twitter filed a lawsuit in federal court seeking to have the restrictions on reporting national security orders held unconstitutional. The case is ongoing as of March 2016.* | | |

| COMPANY | DOJ OPTION 1<br>Separate bands of 0-999 | DOJ OPTION 2<br>Aggregated bands of 0-249 | OTHER REPORTING METHODS & ADDITIONAL INFORMATION REPORTED |
|---|---|---|---|
| **Verizon** | X | | |
| **Wickr** | | | X<br><br>National Security Requests: 0<br>Accounts Associated: 0<br><br>Action to Date: As of the date of this report, Wickr has not yet received an order to keep any secrets that are not in this transparency report as part of a national security request. |
| **Wikimedia Foundation** | *Report does not (specifically) disclose national security orders received.* | | |
| **Yahoo** | X | | |

# INDEX

# INDEX


1. **Adobe**
   https://www.adobe.com/legal/lawenforcementrequests/transparency.html

2. **Amazon**
   http://d0.awsstatic.com/certifications/Information_Request_Report.pdf

3. **AOL**
   http://blog.aol.com/2014/10/28/aol-releases-transparency-report-and-urges-passage-of-the-usa-free

4. **Apple**
   https://www.apple.com/privacy/transparency-reports
   https://www.apple.com/privacy/docs/government-information-requests-20141231.pdf

5. **AT&T**
   http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html
   http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_January_2015.pdf

6. **Automattic**
   http://transparency.automattic.com

7. **Cheezburger**
   http://blog.cheezburger.com/community/cheezburger-inc-2014-transparency-report

8. **Cisco**
   http://www.cisco.com/web/about/doing_business/trust-center/transparency-report.html

9. **CloudFlare**
   https://www.cloudflare.com/transparency2h2014

10. **Comcast**
    http://corporate.comcast.com/images/Third-Comcast-Transparency-Report-2H2014-FINAL-02022015.pdf

11. **CREDO Mobile**
    http://www.credomobile.com/transparency

12. **DigitalOcean**
    https://assets.digitalocean.com/transparency/transparency_report_H12015.pdf

13. **DreamHost**
    https://legal-docs.objects.dreamhost.com/dh-transparency-report-2014.pdf

14. **Dropbox**
    https://www.dropbox.com/transparency

15. **Evernote**
    https://evernote.com/legal/transparency/

16. **Facebook**
    https://govtrequests.facebook.com/

17. **GitHub**
    https://GitHub.com/blog/1987-GitHub-s-2014-transparency-report

18. **Google**
    https://www.google.com/transparencyreport

19. **Inflection**
    http://infl-files.inflection.com.s3.amazonaws.com/Inflection_Transparency_Report_2014.pdf

20. **Internet Archive**
    https://archive.org/about/faqs.php#1007

21. **Kickstarter**
    https://www.kickstarter.com/blog/kickstarter-transparency-report-2014

22. **LinkedIn**
    https://www.linkedin.com/legal/transparency

23. **Lookout**
    https://www.Lookout.com/transparency/ report-2013

24. **Mapbox**
    https://www.mapbox.com/transparency-report/

# INDEX


25. **Medium**
https://medium.com/transparency-report/mediums-transparency-report-438fe06936ff

26. **Microsoft**
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
http://www.microsoft.com/About/CorporateCitizenship/en-us/DownloadHandler.ashx?Id=02-02-00

27. **Nest**
https://nest.com/legal/transparency-report/

28. **Pinterest**
https://help.pinterest.com/en/articles/transparency-report-archive

29. **Reddit**
https://www.reddit.com/wiki/transparency/2014
https://www.redditstatic.com/transparency/2014.pdf

30. **Silent Circle**
https://Silent Circle.com/2015_march_transparency_report

31. **Slack**
https://slack.com/transparency-report

32. **Snapchat**
https://www.Snapchat.com/transparency/02282015.html

33. **Sonic**
https://corp.sonic.net/ceo/2015/03/26/2014-transparency-report/

34. **SpiderOak**
https://spideroak.com/articles/increasing-transparency-alongside-privacy--2014-report

35. **Sprint**
http://goodworks.sprint.com/content/1022/files/CR%20Transaparency%20Report%20Final%20version.pdf
http://goodworks.sprint.com/our-progress/sprint-good-workssm-approach/governance-and-ethics/public-reporting/

36. **Time Warner Cable**
http://help.twcable.com/privacy-safety.html

37. **T-Mobile**
http://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf

38. **Tumblr**
https://www.tumblr.com/transparency
https://secure.static.tumblr.com/uoualm0/gkrnjkdr3/transparencyreport2014jd_letter__5.pdf

39. **Twitter**
https://transparency.twitter.com

40. **Verizon**
http://transparency.verizon.com
http://transparency.verizon.com/themes/site_themes/transparency/Verizon-Transparency-Report-US.pdf

41. **Wickr**
https://wickr.com/category/transparency-report
https://www.wickr.com/wp-content/uploads/2015/06/Wickr-Transparency-Report-June-30-2015.pdf

42. **Wikimedia Foundation**
https://transparency.wikimedia.org/privacy.html

43. **Yahoo**
https://transparency.yahoo.com/government-data-requests/US-JUL-DEC-2014.html