New America Foundation

TRANSPARENCY REPORTING FOR BEGINNERS: MEMO #1
DRAFT 2/26/14

A SURVEY OF

HOW COMPANIES ENGAGED IN TRANSPARENCY REPORTING CATEGORIZE & DEFINE U.S. GOVERNMENT LEGAL PROCESSES DEMANDING USER DATA,

AND IDENTIFICATION OF BEST PRACTICES

OPEN TECHNOLOGY INSTITUTE

HTTP://OTI.NEWAMERICA.ORG

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

Whether you're trying to understand an Internet or telecommunications company's transparency report regarding government requests for customer data, or trying to design a report for your own company, it helps to have a basic understanding of the federal law that regulates law enforcement access to that data: the **Electronic Communications Privacy Act**, or **ECPA**. The ECPA is made up of three component statutes:

The Stored Communications Act (18 U.S.C. § 2701 *et seq.*) regulates government's retrospective access to **stored data**—both the **content** of communications and **non-content** transactional data about those communications, such as information indicating who a communication was to or from, the time it was communicated, and the duration or size of the communication, as well as **basic subscriber information** such as a customer's name, address, billing information, and any identifier such as a username, email address, IP address or the like. The SCA is notoriously complex, but 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);
- 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 without prior court approval and based on the prosecutor's determination that the material sought is relevant to a criminal investigation); and
- 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.

The Wiretap Act (18 U.S.C. § 2511 *et seq.*), sometimes known as "Title III", governs the interception—that is, the prospective or "real-time" wiretapping of the **content** of a target's 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.

The Pen Register Statute (18 U.S.C. §3121 *et seq.*), governs the use of so-called "pen registers" and "trap & trace devices" to capture prospectively or in "real-time" the **non-content** information about a target's communications, such as information indicating who the communication was to or from, the time it was communicated, 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.

The Stored Communications Act also authorizes **National Security Letters** or **NSLs** (18 U.S.C. §2709), secret subpoenas for certain basic subscriber information and non-content transactional information that prosecutors can use to demand information that 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 wide range of court orders for a wide range of types of surveillance and access to data, analogous to the variety orders issued under ECPA for criminal cases but with much more stringent secrecy requirements. Although companies often report specific numbers for specific types of ECPA legal process in their transparency reports, those that report on FISA orders only report a combined number of all of the different types of FISA orders, in ranges of 1000 (e.g., 0-999, 1000-1999, etc.). NSLs are similarly only reported in ranged numbers. Such reporting is permitted by an agreement with the Justice Department that was negotiated in January 2014 by companies that has previously sued in the FISA court for their First Amendment right to report on the national security process they receive (see http://www.justice.gov/opa/pr/2014/January/14-ag-081.html).

HOW DIFFERENT COMPANIES CATEGORIZE DIFFERENT TYPES OF LEGAL PROCESS

The chart on the following page maps how different major Internet and telecommunications companies categorized the various government requests they receive in their last transparency reports. Specifically, we looked at:

- **APPLE's "*Report on Government Information Requests*"**, https://www.apple.com/pr/pdf/131105reportongovinforequests3.pdf, dated 11/5/13, accessed 2/23/14, **and supplemental post "*Update on National Security and Law Enforcement Orders*"**, http://www.apple.com/pr/pdf/140127upd_nat_sec_and_law_enf_orders.pdf, dated 1/27/14, last accessed 2/23/14.
- **AT&T's "*Transparency Report*"**, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html, published 2/18/14 (according to news reports), last accessed 2/23/14.
- **DROPBOX's "*2013 Transparency Report*"**, https://www.dropbox.com/transparency, published 2/11/14 (see attendant blog post at https://blog.dropbox.com/2014/02/our-commitment-to-transparency/), last accessed 2/23/14.
- **FACEBOOK's "*Global Governments Requests Report*"**, https://www.facebook.com/about/government_requests, published 8/27/13 (see attendant blog post at http://newsroom.fb.com/news/699/global-government-requests-report), **and supplemental post "Facebook Releases New Data About National Security Requests"**, http://newsroom.fb.com/News/797/Facebook-Releases-New-Data-About-National-Security-Requests, published 2/3/14, last accessed 2/6/14.
- **GOOGLE's "Transparency Report: Requests for User Information"**, http://www.google.com/transparencyreport/userdatarequests/US/, published 2/3/14 (see attendant blog post at http://googleblog.blogspot.com/2014/02/shedding-some-light-on-foreign.html), last accessed 2/23/14.
- **TUMBLR's "Calendar Year 2013 Law Enforcement Transparency Report"**, http://transparency.tumblr.com/, dated 2/3/14, last accessed 2/23/14.
- **TWITTER's "Transparency Report: Information Requests"**, https://transparency.twitter.com/information-requests/2013/jul-dec, published 2/6/14 (see attendant blog post at https://blog.twitter.com/2014/fighting-for-more-transparency), last accessed 2/23/14.
- **LINKEDIN's "Transparency Report 1H 2013"**. http://help.linkedin.com/app/answers/detail/a_id/41878/ft/eng, last updated 2/3/14 (see attendant blog post at http://blog.linkedin.com/2014/02/03/updated-linkedin-transparency-report-including-requests-related-to-u-s-national-security-related-matters/), last accessed 2/23/14.
- **MICROSOFT's "Law Enforcement Requests Report",** https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/, published 9/27/13, **and supplemental post "Providing additional transparency on US government requests for customer data"**, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data.aspx), published 2/3/14, last accessed 2/23/14.
- **VERIZON's "Transparency Report: US Data"**, http://transparency.verizon.com/us-data, published 1/22/14 (see attendant blog post at http://publicpolicy.verizon.com/blog/entry/verizon-releases-first-transparency-report), last accessed 2/23/14.
- **YAHOO's "Government Data Requests: United States"**, http://info.yahoo.com/transparency-report/us/, published 9/6/13 (see attendant blog post at http://yahoo.tumblr.com/post/60456292987/sharing-our-first-transparency-report), **and supplemental post "More Transparency for U.S. National Security Requests"**, http://yahoo.tumblr.com/post/75496314481/more-transparency-for-u-s-national-security-requests, published 2/3/14, last accessed 2/23/14.

<table>
<tr><th></th><th colspan="8">TYPE OF LEGAL PROCESS</th></tr>
<tr><th>COMPANY</th><th>SEACH WARRANT</th><th>WIRETAP ORDER</th><th>PEN REGISTER ORDER</th><th>18 U.S.C. § 2703(d) ORDER</th><th>SUBPOENA</th><th>EMERGENCY REQUEST</th><th>NATIONAL SECURITY LETTER</th><th>FISA ORDER</th></tr>
<tr><td>Google</td><td rowspan="8">SEARCH WARRANTS</td><td rowspan="2">WIRETAP ORDERS</td><td rowspan="2">PEN REGISTER ORDERS</td><td>“OTHER ORDERS”</td><td rowspan="8">SUBPOENAS</td><td rowspan="6">EMERGENCY REQUESTS</td><td rowspan="3">NSLs</td><td>FISA ORDERS</td></tr>
<tr><td>verizon</td><td>“GENERAL ORDERS”</td><td>not reported</td></tr>
<tr><td>at&t</td><td colspan="2">“COURT ORDERS”, “Real-time”</td><td>“COURT ORDERS”, “Historic”</td><td>FISA ORDERS</td></tr>
<tr><td>tumblr.</td><td colspan="2">not specified*</td><td>“COURT ORDERS”</td><td colspan="2">reports having never received any national security requests</td></tr>
<tr><td>twitter</td><td>not specified*</td><td colspan="2">“COURT ORDERS” (and notes % of pen registers)</td><td colspan="2">not reported</td></tr>
<tr><td>LinkedIn</td><td colspan="2">not specified—possibly “OTHER”? (includes “requests that do not fall within any of the above categories”)</td><td>“COURT ORDERS”</td><td>“OTHER” (includes “emergency requests”)</td><td colspan="2" rowspan="3">NATIONAL SECURITY REQUESTS (NSLs and FISA ORDERS)</td></tr>
<tr><td>Dropbox</td><td colspan="2">not specified*</td><td>“COURT ORDERS”</td><td>not reported</td></tr>
<tr><td>Apple</td><td colspan="6">LAW ENFORCEMENT REQUESTS</td></tr>
<tr><td>Microsoft</td><td colspan="6">LAW ENFORCEMENT REQUESTS (in 9/27/13 report)</td><td>NSLs (in 9/27/13 report & 2/3/14 supplement)</td><td>FISA ORDERS (in 2/3/14 supplement)</td></tr>
<tr><td>facebook
YAHOO!</td><td colspan="8">ALL REQUESTS COMBINED
in primary reports issued in Fall 2013,
supplemental posts with NSL and FISA ORDER numbers reported on 2/3/14</td></tr>
</table>

*** In response to query, company said it did not receive such process in 2013.**

WHAT'S THE BEST PRACTICE FOR CATEGORIZING TYPES OF LEGAL PROCESS?

As the chart above demonstrates, different companies categorize the requests they receive in different ways.

- **Google** is the only company that provides individual reporting on all categories of ECPA requests (search warrants, wiretap orders, pen register orders, D orders, and emergency requests), while also reporting separate NSL and FISA numbers. **Verizon** is just as granular in its categories, but does not report FISA numbers. **AT&T** reports both NSL and FISA numbers, but combines wiretaps and pen registers into a single category of "real-time" court orders such that its is less granular in its categorization than Google or Verizon.

- Four of the companies—**Apple**, **Facebook**, **Microsoft**, and **Yahoo**—currently do not differentiate between different types of law enforcement requests but instead lump them all together, a byproduct of an earlier agreement negotiated with the Justice Department in the summer of 2013 whereby the companies could only report numbers about NSLs and FISA orders if they combined those numbers with all of the law enforcement requests they received (**Google** and **Twitter** chose not to take that deal so they could continue to granularly categorize their law enforcement requests). After a new deal was negotiated with the Justice Department in January 2014, those four companies quickly published supplemental reports or blog posts addressing national security requests. Apple provided a single ranged number for all national security requests combined in a supplemental report on January 27th, while Facebook, Microsoft, and Yahoo all published supplemental blog posts on February 3rd with ranged numbers for both NSLs and FISA orders. However, none of those four companies' most recent transparency reports categorize or specify the number of the different types of law enforcement requests they receive. This lack of granularity will hopefully be remedied in their next reports, expected in the summer.

- Every company that categorizes law enforcement requests has categories for "search warrants" and "subpoenas" received. However, categorization and terminology around other law enforcement court orders and requests differs widely between companies, and represent the clearest need for improvement and opportunity for standardization. Many companies have categories for "court orders" or "other orders" or "other" requests that often cover a differing range of orders or requests, sometimes including emergency requests. Most of the time, references to "court orders" appear to refer to—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.

- Notably, the chart does not include every company that has issued a transparency report. **Sonic.net**'s transparency report (http://corp.sonic.net/ceo/2013/05/24/2012-transparency-report/) has only a single undefined category for government requests, "law enforcement court orders". **SpiderOak**'s transparency report (https://spideroak.com/blog/20130404171036-increasing-transparency-alongside-privacy-2013-report) divides government requests into federal law enforcement and state law enforcement requests but otherwise doesn't categorize them. **CREDO Mobile** (http://www.credomobile.com/misc/transparency.aspx) doesn't categorize requests but instead individually describes each of the few requests it receives. **LeaseWeb** (http://blog.leaseweb.com/2013/04/11/leaseweb-first-hosting-provider-worldwide-to-launch-law-enforcement-transparency-report/) isn't a US company and therefore doesn't specifically address different types of US requests. Due to these reports' unique and sometimes unclear nature, they aren't included in the chart.

BEST PRACTICE: GOOGLE

Google's report represents the current best practice when it comes to clear and granular categorization of legal process; Verizon is nearly as granular, except for its failure to include or define FISA orders. We encourage adoption of these companies' categorizations as a standard, both for those already engaged in reporting and those issuing their first reports.

HOW ARE COMPANIES CURRENTLY DEFINING DIFFERENT TYPES OF LEGAL PROCESS?

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, this is how they define those categories.

SEARCH WARRANTS

- **Google** defines "Search Warrant" on its main transparency report page as "An order issued by a judge under ECPA based on a demonstration of probable cause that compels the production of information," and also has an extensive legal process FAQ further describing search warrants (https://www.google.com/transparencyreport/userdatarequests/legalprocess/):
    - The threshold is higher still for an ECPA search warrant [compared to an ECPA D Order]. 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. While many warrants seek the same types of information that can also be obtained through a general order or subpoena, most warrants we received in 2013 sought stored content or location information."
    - *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.
    - *What is the difference between stored content and non-content?* "Stored content" refers to communications or other data that our users create and store through our services, such as text messages, email or photographs. We require a warrant before disclosing stored content to law enforcement, absent an emergency involving the danger of death or serious physical injury. 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.
- **AT&T:** "Search Warrants are signed by a judge, and they require law enforcement to show evidence to the court that there is probable cause to believe the information requested by the warrant is evidence of a crime. They are used only in criminal cases, and they are almost always required to obtain real-time location information."
- **Tumblr:** "Search warrants may be issued if a reviewing judge or magistrate concludes that there is "probable cause" to believe that a particular account may contain information related to a crime. Search warrants are generally harder to obtain than 2703(d) orders or subpoenas. Under U.S. law, we may disclose the same account data described above, as well as blog content, in response to a lawful search warrant. Blog content includes the posts made to a blog, both public or private. Posts can be one of Tumblr's seven post types, including text, audio, images, or videos."
- **Twitter:** "Search Warrants": As prescribed by the Fourth Amendment, warrants typically require the most judicial scrutiny before they are issued, including a showing of probable cause and a judge's signature. A properly executed warrant is required for the disclosure of the contents of communications (e.g., Tweets, DMs)."
- **LinkedIn**: "Search Warrants require the government to demonstrate 'probable cause' and are generally issued by a judge. The standard applicable to a search warrant is higher than that applicable to a subpoena."

- **Dropbox:** "Search warrants": "Search warrants require judicial review, a showing of probable cause, and must meet specificity requirements regarding the place to be searched and the items to be seized. Search warrants may be issued by local, state or federal governments, and may only be used in criminal cases. In response to valid search warrants, we produce non-content and content information."

WIRETAP ORDERS

- **Google** defines a "Wiretap Order" on its main transparency report page as "An order issued by a judge under ECPA for real-time disclosure of content," and also has an extensive legal process FAQ further describing search warrants (https://www.google.com/transparencyreport/userdatarequests/legalprocess/):
  - 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.
  - Statistics about federal and state wiretaps are available here.
- **Verizon:** "Wiretaps [are] where law enforcement accesses the content of a communication as it is taking place."
  - *What is a 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.
  - *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.
- **AT&T:** "wiretap orders... allow law enforcement to monitor phone calls or text messages while they are taking place" (described as a subcategory of "court order").

PEN REGISTER ORDERS

- **Google** defines "a pen register order" on its main transparency page as "An order issued under ECPA for real-time disclosure of dialing, routing, addressing and signaling information, but not content," and also has an extensive legal process FAQ further describing such orders (https://www.google.com/transparencyreport/userdatarequests/legalprocess/):
  - 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.

- **Verizon:** "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."
    - *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.
    - *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 -- that the information likely to be obtained is relevant to an ongoing criminal investigation.
- **AT&T:** "pen register/trap and trace orders...provide information and phone numbers for all calls as they are made or received." (described as a subcategory of "court order").
- **Twitter:** "PRTT orders: Originally developed to obtain phone numbers from telco providers, a PRTT order (in the context of Twitter) provides law enforcement with legal authority to obtain IP address records from the account identified in the order, generally for 60 days."

OTHER COURT ORDERS (*i.e.* and *e.g.*, 18 USC § 2703(D) ORDERS)

- **Google** defines "Other Court Orders" on its main transparency page as "Miscellaneous orders for user information, such as ECPA 2703(d)," and also has an extensive legal process FAQ further describing "ECPA Court Orders" (https://www.google.com/transparencyreport/userdatarequests/legalprocess/):
    - Unlike an ECPA subpoena, obtaining an ECPA court order requires judicial review. To receive an ECPA court order, a government agency must present specific facts to a judge or magistrate demonstrating that the requested information is relevant and material to an ongoing criminal investigation.
    - With such a court order, a government agency can obtain the same information as a subpoena, plus 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. An ECPA court order is available only for criminal investigations.
- **Verizon:** "General Orders": "We use the term 'general order' to refer to an order other than a wiretap order, warrant, or pen register trap and trace order. Almost half of all general orders required us to release the same types of basic information that could also be released pursuant to a subpoena. We do not provide law enforcement any stored content (such as text messages or email) in response to a general order."
    - *What are the different showings that law enforcement has to make for the different orders?* A general order requires law enforcement to offer specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation. In federal court, such orders are authorized under 18 U.S.C. § 2703(d).
- **AT&T:** "Court Orders are signed by a judge. They are used in both criminal and civil cases 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 information. This can include wiretap orders, which allow law enforcement to monitor phone calls or text messages while they are taking place, or pen register/"trap and trace" orders, which provide information and phone numbers for all calls as they are made or received."
- **Tumblr:** "Court orders for user data may be issued under various U.S. federal and state laws, such as section 2703(d) of the Electronic Communications Privacy Act, a federal privacy law. Court orders are issued by judges and are generally harder to obtain than subpoenas. If we

receive a lawful 2703(d) order, we may disclose the same account data described above with respect to subpoenas, plus an additional category of account data: the IP address used to post a particular piece of content."

- **Twitter:** "Court Orders": "Unlike subpoenas, court orders must be issued by an appropriate court and signed by a judge."
- **LinkedIn:** "Court orders vary depending on the circumstances and the issuing Court and jurisdiction. Many of the Court orders LinkedIn receives are issued pursuant to 18 USC § 2703(d), a provision of the Electronic Communications Privacy Act (ECPA). To obtain such an order, the government must demonstrate specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and material to an ongoing investigation. This standard is higher than that applicable to subpoenas but lower than that applicable to search warrants."
- **Dropbox:** "Court orders: Court orders are issued by judges and may take a variety of forms, such as a 2703(d) order under the Electronic Communications Privacy Act, in both civil and criminal cases. 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."

SUBPOENAS

- **Google** defines "Subpoena" on its main transparency page as "A formal request issued under ECPA for the production of information that may not involve a judge," and also has an extensive legal process FAQ further describing subpoenas (https://www.google.com/transparencyreport/userdatarequests/legalprocess/):
    - 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:** "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. More than 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."
    - *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.
    - *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.

- *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:** "Subpoenas don't usually require the approval of a judge and are issued by an officer of the court. They are used in both criminal and civil cases, typically to obtain written business documents such as calling records."
- **Tumblr:** "Subpoenas are the most common requests we receive. They generally don't require a judge's review. Under U.S. law, we may disclose limited account data in response to a lawful subpoena. Account data includes registration email address, how long a Tumblr account has been registered, and login IP addresses. Account data does *not* include the posts made to a blog, whether public or private. Because Tumblr doesn't collect real names or addresses, we don't (and can't) provide this information in response to a subpoena."
- **Twitter**: "Subpoenas are the most common form of legal process issued under the Stored Communications Act; they do not generally require a judge's sign-off and usually seek basic subscriber information, such as the email address associated with an account and IP logs."
- **LinkedIn**: "Subpoenas may be issued for information that is reasonably relevant to the general subject matter of a pending investigation. They are typically pre-signed by a court clerk and are issued by prosecutors without the involvement of a judge."
- **Dropbox: "**Subpoenas include any legal process from law enforcement where there is no legal requirement that a judge or magistrate review the legal process. Local, state and federal government authorities may use subpoenas in both criminal and civil cases and subpoenas are typically issued by government attorneys or grand juries. We do not produce content information in response to subpoenas."

EMERGENCY REQUESTS

- **Google** defines an "Emergency Request" on its main transparency reporting page as "A request from a government agency seeking information to save the life of a person who is in peril or prevent serious physical injury," and also has an extensive legal process FAQ further describing what constitutes an emergency case (https://www.google.com/transparencyreport/userdatarequests/legalprocess/):
  - 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 Requests": "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 regarding particular 9-1-1 calls from the public. Calls for emergency services, such as police, fire or ambulance, are answered in call centers throughout the country, known as PSAPs. 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." These are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies."

- **Tumblr:** "in the interest of public safety and, in particular, the safety of our users, we may voluntarily disclose user information to appropriate government officials if we believe it's necessary to prevent an emergency involving death or serious physical injury. In 2013, the vast majority of these voluntary emergency disclosures originated from members of the Tumblr community who notified government officials that another user might be attempting to commit suicide. In such cases, we may disclose limited information, such as an IP address, so that officials can locate the user and provide him or her with immediate assistance."
- **Twitter:** "Emergency Disclosure Requests: Twitter evaluates emergency disclosure requests on a case-by-case basis in compliance with 18 U.S.C. § 2702(b)(8). If we receive information that gives us a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, we may provide information necessary to prevent that harm, if we have it."

NATIONAL SECURITY LETTERS

- **Google** describes on its main transparency report page that "National Security Letters are requests 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," and also has an extensive FAQ section describing NSLs (http://www.google.com/transparencyreport/userdatarequests/faq/#what_is_an_nsl):
    - *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. 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.
    - *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.
    - *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.
    - *Does Google notify users when it receives NSLs asking for information about their accounts?* It's Google's practice to notify users about legal demands when appropriate, unless prohibited by law or court order. The FBI has the power to prohibit the recipient of an NSL from disclosing the fact that it has received an NSL, by certifying that disclosure may result in "a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person."
- **Verizon: "**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."
    - *What is an NSL?* 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."

- *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."
- *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."

- **AT&T:** "National Security Letters are subpoenas issued by the Federal Bureau of Investigation in regard to counterterrorism or counterintelligence. These subpoenas are limited to non-content information, such as a list of phone numbers dialed or subscriber information."
- **Tumblr:** "National Security Letters [are] FBI-issued requests for subscriber information."

FISA ORDERS

- **Google** describes on its main transparency report page that "FISA requests are court orders that can require U.S. companies to hand over personal information in national security investigations," and also has an extensive fact section describing FISA (http://www.google.com/transparencyreport/userdatarequests/US/#FISA_requests).
  - *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.
  - *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. ¶ 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.
  - *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.
  - *Does Google notify users when/if it receives FISA requests about their accounts?* Organizations like Google that receive FISA requests are prohibited from notifying users.
  - *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."
- **AT&T:** "Court orders issued pursuant to FISA direct communications providers to respond to government requests for content and non-content data related to national security investigations, such as international terrorism or espionage."

- **Tumblr: "**Foreign Intelligence Surveillance Act ("FISA") orders [are] orders issued in classified court proceedings, requiring companies to provide user information in national security investigations."
- **Microsoft** reports FISA Order data using the following definitions:
    - *FISA Orders Seeking Disclosure of Content:* This category would include any FISA electronic surveillance orders (50 U.S.C. § 1805), FISA search warrants (50 U.S.C. § 1824), and FISA Amendments Act directives (50 U.S.C. §1881) that were received or active during the reporting period.
    - *FISA Orders Requesting Disclosure of Non-Content:* This category would include any FISA business records (50 U.S.C. § 1861), commonly referred to as 215 orders, and FISA pen register and trap and trace orders (50 U.S.C. § 1842) that were received or active during the reporting period.

"OTHER"/MISCELLANEOUS/UNCLEAR/CATCH-ALL CATEGORIES

- **LinkedIn**: "Other" category includes requests that do not fall within any of the above categories. Examples include emergency requests."
- **Twitter**: "Other": "Requests from law enforcement that do not fall in any of the above categories. Examples include exigent emergency disclosure requests (which we now breakout in the table above) and other requests received for account information without valid legal process." (This category of requests—those lacking valid process—is not represented in the chart above but would be a worthwhile category for all providers to offer.)

ADDITIONAL INFORMATION IN LAW ENFORCEMENT GUIDES

Some companies also have guidelines or principles or FAQS regarding handling law enforcement requests, separate from or in addition to their transparency reports, that may contain information regarding how they define or respond to different types of legal process, *e.g.*:

- Dropbox: https://www.dropbox.com/transparency/principles
- Google: https://www.google.com/transparencyreport/userdatarequests/legalprocess/
- Facebook: https://www.facebook.com/safety/groups/law/guidelines/
- LinkedIn: http://help.linkedin.com/ci/fattach/get/2730181/0/filename/LinkedIn%20Law%20Enforcement%20Guidelines.pdf
- Tumblr: http://www.tumblr.com/docs/en/law_enforcement
- Twitter: https://support.twitter.com/articles/41949-guidelines-for-law-enforcement
- Yahoo: http://info.yahoo.com/transparency-report/us/law-enforcement-guidelines/

BEST PRACTICE: GOOGLE & VERIZON

Google and Verizon tie for first place. Google has the most granular and complete definitions for each category of legal process, including FISA orders, but those definitions are found in a separate "legal process" FAQ page linked to from the main transparency page, not on the same page as the reported data. Verizon's report does not include or define FISA orders, and its definitions are not quite as detailed, but that is in part due to the fact that the definitions are necessarily shorter so that they fit within and are well-integrated into the design of the main report page, and are more readily readable then Google's definitions.

COMING SOON!

MEMO #2:

DEFINING CATEGORIES OF REQUESTED DATA AND RELATED SUBCATEGORIES OF REQUESTS, AND WHICH COMPANIES SHARE WHICH DATA IN REPONSE TO WHICH REQUESTS