verizon

Transparency Report 2H 2017

verizon

United States report

The table below sets out the number of subpoenas, orders, warrants and emergency requests we received from federal, state or local law enforcement in the United States in the second half of 2017. The table presents data for the past three years; data from prior periods can be found by clicking on the Archive tab at the top of the page. The total number of demands (and the number of subpoenas, orders, warrants and emergency requests) in the second half of 2017 were generally comparable with the number of demands we received in prior six-month periods.

The vast majority of these various types of demands relate to our consumer customers; we receive relatively few demands regarding our enterprise customers. We do not release customer information unless authorized by law, such as a valid law enforcement demand or an appropriate request in an emergency involving the danger of death or serious physical injury.

Law Enforcement Demands for Customer Data — United States

	1st Half of 2014	2nd Half of 2015	1st Half of 2016	2ndHalf of 2016	1st Half of 2017	1st Half of 2017
Subpoenas	69,524	65,663	67,433	60,408	68,237	68,237
Total orders	37,230	33,813	67,433	31,443	32,337	32,337
General Orders	33,138	30,568	67,433	28,192	28,374	28,374
Pen Registers/ Trap & Trace Orders	3,325	2,678	67,433	2,601	3,241	3,241
Wiretap Orders	767	567	656	650	722	722
Warrants	15,081	14,248	11,798	10,315	10,721	10,721
Emergency Requests From Law Enforcement	27,975	25,844	23,394	10,315	10,721	10,721
Total	**149,810**	**139,568**	**135,786**	**129,249**	**138,773**	**138,773**

We also received National Security Letters and FISA Orders; we address them in a separate table at the bottom of this Transparency Report.

verizon

Verizon has teams that carefully review each demand we receive. We do not produce information in response to all demands we receive. In the second half of 2017 we rejected more than three percent of the demands we received; that is, we rejected almost three percent of the subpoenas we received and almost four percent of the warrants and orders we received. 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.

There are a number of additional reasons why we might not produce some or all of the information sought by a demand, although we do not consider these "rejected" demands and do not calculate the number of times these occur. e we have no need to collect or were older than our retention period. Moreover, if a demand is overly broad, we will not produce any information, or will seek to narrow the scope of the demand and produce only a subset of the information sought. Additionally, it is not uncommon for us to receive legal process and in response produce some information, but not other information. For instance, we may receive a subpoena that properly seeks subscriber information, but also improperly seeks other information, such as stored content, which we cannot provide in response to a subpoena; while we would provide the subscriber information (and thus would not consider this a rejected demand), we would not provide the other information. We include all demands we receive in our table above, whether we provided data in response or not.

Which Verizon services does this Transparency Report cover?
The figures in this Report include demands for customer data regarding our Verizon wireline services, such as phone, Internet or television, and our Verizon Wireless services and telematics. This report does not include statistics for AOL Inc., which Verizon acquired in June 2015, or Yahoo!, which Verizon acquired in June 2017. Yahoo! and AOL have formed Oath, which will issue a separate transparency report.

Does this Transparency Report include information on the number of national security orders you receive?
Yes.

Does Verizon charge law enforcement for providing data?
In some instances, federal and most state laws authorize providers to charge a reimbursement fee for responding to law enforcement demands for records or to recoup reasonable expenses in complying with a wiretap order or pen register or trap and trace order. In the majority of instances, however, we do not seek reimbursement for responding to law enforcement requests. We do not charge for responding to emergency requests and do not charge for responding to most subpoenas. When we do charge a reimbursement fee, our fees are permitted by law or court order and seek to recoup only some of our costs.

Does Verizon also receive requests for data in civil cases?
Yes, we do. Requests in civil cases comprise a small percentage of the total requests we receive. This report focuses on requests from law enforcement.

verizon

Will Verizon issue future transparency reports?
Yes, on a semi-annual basis.

What obligations to report on demands already apply to the United States government?
Federal law already places substantial reporting requirements on federal and state governments.
Each year the United States Attorney General and the principal prosecuting attorney for each state have to report the number of applications for wiretap orders, the number of orders granted, the types of communications intercepted, the number of persons whose communications were intercepted and the numbers of arrests and convictions resulting from such interceptions. That information is summarized for Congress. See 18 U.S.C. § 2519(2),(3). Similarly, the Attorney General must make detailed annual reports to Congress on the number of pen registers and trap and trace orders. See 18 U.S.C. § 3126.
The Attorney General also has to report to Congress each year regarding information obtained in emergencies, in some contexts. See 18 U.S.C. § 2702(d). And the Director of the FBI has to report twice each year to Congress regarding the number of National Security Letters issued. See 18 U.S.C. § 2709(e).

Subpoenas

We received 61,211 subpoenas from law enforcement in the United States in the second half of 2017. 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.

In the second half of 2017, the 61,211 subpoenas we received sought information regarding 106,128 information points, such as a telephone number, used to identify a customer. These customer identifiers are also referred to as "selectors." On average, each subpoena sought information about 1.7 selectors. 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. We have also determined that during the second half of this year, just like during the prior periods, approximately 75 percent of the subpoenas we received sought information on only one selector (and thus only one customer), and over 90 percent sought information regarding three or fewer selectors (and thus three or fewer customers).

verizon

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).

Orders

We received 32,891 court orders in the second half of 2017. These court orders must be signed by a judge, indicating that the law enforcement officer has made the requisite showing required under the law to the judge. The orders compel us to provide some type of information to the government.

General Orders. Most of the orders we received – 28,817 – were "general orders." We use the term "general order" to refer to an order other than a wiretap order, warrant, or pen register or trap and trace order. We continue to see that many of these general orders require 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.

"Pen/Trap" Orders and Wiretap Orders. A small subset – 4,074 – of the orders we received in the first half of 2017 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.

We received 3,383 court orders to assist with pen registers or trap and traces in the second half of 2017, although generally a single order is for both a pen register and trap and trace. Far less frequently, we are required to assist with wiretaps, where law enforcement accesses the content of a communication as it is taking place. We received 691 wiretap orders in the second half of 2017.

verizon

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 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.
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).
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.

Warrants

We received 10,631 warrants in the second half of 2017. 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. A warrant may be used to obtain stored content (such as text message content or email content), location information or more basic subscriber or transactional 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.

Content and location information

Content. We are compelled to provide contents of communications to law enforcement relatively infrequently. Under the law, law enforcement may seek communications or other content that a customer may store through our services, such as text messages or email. 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. During the second half of 2017, we received 4,527 warrants for stored content.

Location information. Verizon only produces location information in response to a warrant or order; we do not produce location information in response to a subpoena. The laws in some areas of the country require law enforcement to obtain a warrant to get location information, but the laws in other areas permit law enforcement to obtain a court order. In either scenario, the demand we receive for location information is approved by a judge. In the second half of 2017, we received approximately 21,106 demands for location data: about three-quarters of those were through orders and one-quarter were through warrants.

In addition, we received approximately 6,886 warrants or court orders for "cell tower dumps" in the second half of this year. In order to try to identify a suspect of a crime, the government may apply to a court for a warrant or order compelling us to provide a "dump" of the phone numbers of all devices that connected to a specific cell tower or site during a given period of time. This tool is being used much more frequently by law enforcement. We previously reported that in 2013 we received approximately 15,756 warrants or orders for cell tower dumps; we received 15,756 warrants or orders for cell tower dumps in 2017.

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 (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

verizon

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.

In the second half of 2017, we received 28,125 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury. We also received 15,507 emergency requests from PSAPs related to particular 9-1-1 calls from the public for emergency services during that same period.

National security demands

The table below sets forth the number of national security demands we received in the applicable period. Under section 603 of the USA Freedom Act we are now able to report the number of demands in bands of 500.

	Jan. 1, 2015 – June 30, 2015	July 1, 2015 – Dec. 31, 2015	Jan. 1, 2016 – June 30, 2016	July 1, 2016 – Dec. 31, 2016	Jan. 1, 2017 – June 30, 2017	July 1, 2017 – Dec 31, 2017
National Security Letters	501-999	1-499	1-499	2-499	1-499	500-999
Number of customer selectors	2000-2499	500-999	500-999	1000-1499	1500-1999	1500-1999
FISA Orders (Content)	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	1500-2999	1000-1499	2000-2499	2000-2499	1500-1999	*
FISA Orders (Non-Content)	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	0-499	0-499	0-499	0-499	0-499	*
* The government has imposed a six month delay for reporting this data.						

verizon

National Security Letters

In the second half of 2017, we received between 500 and 999 NSLs from the FBI. Those NSLs sought information regarding between 1500 and 1999 "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.

National Security Letters typically prohibit a recipient, such as Verizon, from disclosing to any other person that an NSL was received or that the recipient provided information in response to it. Until recently, such non-disclosure requirements applied indefinitely. The USA Freedom Act, however, required the FBI to periodically review if each NSL recipient could be relieved of the non-disclosure requirements. To that end, we have recently received letters from the FBI advising that the non-disclosure requirements of seven NSLs – received in May 2013, May 2014 (two), July 2014 (two), August 2016 and April 2017 – are no longer applicable.

We therefore can now disclose that we complied with each NSL by provided name, address, dates of service and/or toll billing records, as authorized by the relevant statute. Th e May 2013 NSL sought information regarding two customer selectors and one of the July 2014 NSLs souhgt information regarding two customer selectors. The other five NLSs sought information regarding only one customer selectr. Moreover, where applicable, we have revised the table above to reflect receipt of these NSLs.

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.

verizon

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.

FISA Orders

The government requires that we delay the report of any orders issued under the Foreign Intelligence Surveillance Act for six months. Thus, at this time, the most recent FISA information we may report is for the first half of 2017.

Content

From January 1, 2017 through June 30, 2017, we received between 0 and 499 FISA orders for content. Those orders targeted between 1,500 and 1,999 "customer selectors" used to identify a Verizon customer.

Non-Content

From January 1, 2017 through June 30, 2017, we received between 0 and 499 reportable FISA orders for non-content. Some FISA orders that seek content also seek non-content; we counted those as FISA orders for content and to avoid double counting have not also counted them as FISA orders for non-content. Those orders targeted between 0 and 499 "customer selectors."

What is a "FISA Order"?
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.

What is a "FISA Order for Content"?
A FISA order for content is an order that compels a service provider to give the government the content of certain communications carried on the provider's networks. A FISA order for content could compel the provider to intercept voice communications or provide the government with stored content. For example, the government could seek a FISA electronic surveillance order (pursuant to 50 U.S.C. §1805 or §1881a) or search order (pursuant to 50 U.S.C. §1824) from the FISA court to compel content from a provider.

verizon

What is a "FISA order for non-content?"

A FISA order for non-content is an order that compels a service provider to produce call detail records or similar "transactional" information about communications carried on the provider's networks, but does not require the provider to produce any content. A FISA pen register or trap and trace order and a so-called section "215 order" are FISA orders for non-content. For example, the government could seek a FISA pen register or trap and trace order (pursuant to 50 U.S.C. §1842) from the FISA court to compel a provider to produce routing information. The government may seek a section 215 order (pursuant to 50 U.S.C. §1861) to obtain the types of information obtained through a grand jury subpoena or a court order.