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 2018. 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 2018 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

1H 2016	1H 2016	2H 2016	1H 2017	2H 2017	1H 2018	2H 2018
Subpoenas	67,433	60,408	68,237	61,211	69,596	64,017
Total Orders	33,161	31,443	32,337	32,891	30,361	28,098
General Orders	29,635	28,192	28,374	28,817	29,929	24,349
Pen Registers/Trap & Trace Orders	2,870	2,601	3,241	3,383	3,787	3,163
Wiretap Orders	656	650	722	691	645	586
Warrants	11,798	10,315	10,721	10,631	13,552	14,543
Emergency Requests From Law Enforcement	23,394	27,083	27,478	28,125	31,239	33,001
Total	**139,568**	**135,786**	**138,773**	**132,858**	**144,748**	**139,659**

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

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 2018 we rejected more than three percent of the demands we received; that is, we rejected almost three percent of the subpoenas we received and more than 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. We often receive demands seeking information about a phone number serviced by a different provider. And, we regularly receive demands seeking data that we do not have – perhaps the data sought were of a type 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.

Subpoenas

We received 64,017 subpoenas from law enforcement in the United States in the second half of 2018. 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 2018, the 64,017 subpoenas we received sought information regarding 108,573 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 2018, 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).

Orders

We received 28,098 court orders in the second half of 2018. 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 – 24,349 – 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 – 3,749 – of the orders we received in the second half of 2018 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 3,163 court orders to assist with pen registers or trap and traces in the second half of 2018, 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 586 wiretap orders in the first second of 2018.

Warrants

We received 14,543 warrants in the second half of 2018. 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.

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 2018, we received 10,038 warrants for stored content.

Location information. In the second half of 2018, we received 12,397 warrants based on probable cause for location data. In addition, we received 1,320 warrants or court orders for "cell tower dumps" in the second half of the year.

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 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 2018, we received 33,001 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury. We also received 17,515 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, 2016 – Jun. 30, 2016	**Jul. 1, 2016– Dec. 31, 2016**	**Jan 1, 2017– Jun. 30, 2017**	**July 1, 2017– Dec. 31, 2017**	**Jan 1, 2018– Jun. 30, 2018**	**Jul. 1, 2018– Dec. 31, 2018**
National Security Letters	1-499	5-499	1-499	501-999	1-499	0-499
Number of customer selectors	500-999	1000-1499	1500-1999	1500-1999	2000-2499	2000-2499
FISA Orders (Content)	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	2000-1499	2000-2499	1500-1999	2000-2499	2000-2499	*

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.

National Security Letters

In the second half of 2018, we received between 500 and 999 NSLs from the FBI. Those NSLs sought information regarding between 2500 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.

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 three NSLs – received in September 2014, March 2015 and August 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. The September 2014 NSL sought information regarding three customer selectors the other two NSLs sought information regarding one customer selector. Moreover, where applicable, we have revised the table above to reflect receipt of these NSLs.

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 2018.

From January 1, 2018 through June 30, 2018, we received between 0 and 499 FISA orders for content. Those orders targeted between 2,000 and 2,499 “customer selectors” used to identify a Verizon customer.

From January 1, 2018 through June 30, 2018, 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.”