Verizon's Transparency Report for the 1st Half of 2020

Verizon's Transparency Report presents the number of demands we received from law enforcement in the United States and other countries in which we did business in the first half of 2020

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 first half of 2020. 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 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.

The total number and types of demands we receive continues to be fairly stable as compared to prior six-month periods. We have generally been seeing an increase in the number of Warrants and a decrease in the number of Orders. That is due in part to the Supreme Court requiring law enforcement to show probable cause to obtain location information. And, instead of automatically classifying any legal process to provision a Pen Register, Trap and Trace or Wiretap as an Order, if the legal process is captioned as a Warrant, we now classify such process as a Warrant (instead of an Order). In addition, we have moved to a new system for tracking legal process, which we believe will help us report with more accuracy. For instance, we now have a better method for excluding duplicates. We also discovered that in prior reports we errantly double counted some types of orders.

Law Enforcement Demands for Customer Data — United States

	1H 2017	2H 2017	1H 2018	2H 2018	1H2019	2H2019	1H2020
Subpoenas	68,237	61,211	69,596	64,017	68,192	64,136	66,773
Orders	24,448	24,767	21,520	20,614	19,269	12,586	5760
Pen Register/ Trap & Traces	3,241	3,383	3,787	3,163	3,753	3,866	3721
Wiretaps	722	691	645	586	585	525	612
Warrants	10,721	10,631	13,552	14,543	13,870	18,721	16,818
Emergency Requests From Law Enforcement	27,478	28,125	31,239	33,001	30,365	33,518	34,868
Total	**134,847**	**128,808**	**140,339**	**135,924**	**136,034**	**133,352**	**128,552**

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 first half of 2020 we rejected three percent of the demands we received; that is, we rejected about three percent of the subpoenas we received and about five 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 66,773 subpoenas from law enforcement in the United States in the first half of 2020. 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 first half of 2020, the 66,773 subpoenas we received sought information regarding 136,649 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 2.0 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 first half of 2020, approximately 70 percent of the subpoenas we received sought information on only one selector (and thus only one customer), and about 90 percent sought information regarding three or fewer selectors (and thus three or fewer customers).

Orders

A court order must be signed by a judge, indicating that the law enforcement officer has made the requisite showing required under the law. An order compels us to provide some type of information to the government. We do not provide law enforcement any content (such as text messages or email) in response to an order.

General Orders. Most of the orders we received in the first half of 2020—5,760—were "general orders." We use the term "general order" to refer to an order other than legal process asking us to provision a wiretap, pen register or trap and

trace, or a warrant. 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.

"Pen/Traps" and Wiretaps. We received 4,333 demands in the first half of 2020 requiring us to provide access to data in real-time. These are commonly referred to as pen register orders, trap and trace orders or wiretap orders, although, as noted above, an increasing number of them are now being captioned as warrants. 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 received 3,721 warrants or court orders to assist with pen registers or trap and traces in the first half of 2020, although generally a single demand 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 612 warrants or orders for wiretaps in the first half of 2020.

Warrants

We received 16,818 warrants in the first half of 2020. 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.

In the first half of 2020, we received a total of 25,266 orders and warrants. They sought data regarding 60,097 information points, such as a telephone number, used to identify a customer. These customer identifiers are also referred to as "selectors." On average, each order or warrant sought information about 2.4 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 an order or warrant seeking information about multiple selectors was actually seeking information about just one customer. We have also determined that during the first half of 2020, slightly more than 70 percent of the orders and warrants we received sought information on only one selector (and thus only one customer), and almost 90 percent sought information regarding three or fewer selectors (and thus three or fewer customers).

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 first half of 20209, we received 9,260 warrants for stored content.

Location information. In the first half of 2020, we received 14,936 warrants based on probable cause for location data. In addition, we received 1,611 warrants or court orders for "cell tower dumps" in the first half of 2020. 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.

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 first half of 2020, we received 34,868 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury. We also received 12,357 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, 2017–Jun. 30, 2017	**July 1, 2017–Dec. 31, 2017**	**Jan 1, 2018–Jun. 30, 2018**	**Jul. 1, 2018–Dec. 31, 2018**	**Jan 1, 2019–Jun. 30, 2019**	**June 30, 2019 –Dec. 31 2019**	**Jan. 1, 2020–Jun. 30, 2020**
National Security Letters	1-499	501-999	2-499	0-499	0-499	0-499	0-499
Number of customer selectors	1500-1999	1500-1999	2000-2499	2000-2499	1500-1999	3500-3999	1000-1499
FISA Orders (Content)	0-499	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	1500-1999	2000-2499	2000-2499	1500-1999	1000-1499	1000-1499	*
FISA Orders (Non-Content)	0-499	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	0-499	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 first half of 2020, we received between 0 and 499 NSLs from the FBI. Those NSLs sought information regarding between 1000 and 1499 “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 a letter from the FBI advising that the non-disclosure requirement of an NSL—received in March 2014—is no longer applicable.

We therefore can now disclose that we complied with that NSL by providing the name, address, dates of service and/or toll billing records, as authorized by the relevant statute. The NSL sought information regarding one customer selector.

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 2019.

Content

From July 1, , 2019 through December 31, 2019, we received between 0 and 499 FISA orders for content. Those orders targeted between 1,000 and 1,499 “customer selectors” used to identify a Verizon customer.

Non-content

From July 1, 2019 through December 31, 2019, 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.”