Verizon's Transparency Report for the First Half of 2015

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 2015. The number of demands in the first half of 2015 were generally comparable with the number of demands we have 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

	2013 (Full Year)	**Half of 2013 ***	**1st Half of 2014**	**2nd Half of 2014**	**1st Half of 2015**
Subpoenas	164,184	82,092	72,342	65,816	69,524
Total Orders	70,665	35,333	37,327	33,453	37,230
General Orders	62,857	31,429	33,313	29,656	33,138
Pen Registers/ Trap & Trace Orders	6,312	3,156	3,300	3,078	3,325
Wiretap Orders	1,496	748	714	719	767
Warrants	36,696	18,348	14,977	13,050	15,081
Emergency Requests From Law Enforcement	50,000 (approx)	25,000 (approx)	24,257	26,237	27,975
Total	**321,545**	**160,773**	**148,903**	**138,656**	**149,810**

** In our first Transparency Report (published in January 2014), we reported on the full year for 2013. Since that Report, we have reported data based on half-year periods. To aid the comparison between the half-year numbers we have reported since 2013 and the full-year numbers we reported in 2013, we have simply halved the 2013 numbers in the table.*

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 2015, we rejected as invalid approximately three percent of the demands 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 would 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.

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.

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.

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 69,524 subpoenas from law enforcement in the United States in the first half of 2015. 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 2015, the 69,524 subpoenas we received sought information regarding 121,256 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 1.75 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 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).

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 37,230 court orders in the first half of 2015. 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 – 33,138 – 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 – 4,092 – of the orders we received in the first half of 2015 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 3,325 court orders to assist with pen registers or trap and traces in the first half of this year, 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 767 wiretap orders in the first half of 2015.

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 15,081 warrants in the first half of 2015. 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 first half of 2015, we received 5,944 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 first half of this year, we received approximately 21,800 demands for location data: as in the past, about two-thirds of those were through orders and one-third were through warrants. In addition, we received approximately 3,410 warrants or court orders for "cell tower dumps" in the first half of this year. In such instances, the warrant or court order compelled us to identify the phone numbers of all phones that connected to a specific cell tower 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 2015, we received 27,975 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury. We also received 11,242 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. We note that while we are able to provide some information about national security orders that directly relate to our customers, reporting on other matters, such as any orders we may have received related to the bulk collection of non-content information, remains prohibited.

	Jan. 1, 2013 –	July 1, 2013 – Dec.	Jan. 1, 2014 –	July 1, 2014 – Dec.	July 1, 2015 –

	June 30, 2013	31, 2013	June 30, 2014	31, 2014	June 30, 2015
National Security Letters	0-999	0-999	0-999	0-999	0-999
Number of customer selectors	2000-2999	2000-2999	2000-2999	2000-2999	2000-2999
FISA Orders (Content)	0-999	0-999	0-999	0-999	*
Number of customer selectors	4000-4999	3000-3999	3000-3999	2000-2999	*
FISA Orders (Non-Content)	0-999	0-999	0-999	0-999	*
Number of customer selectors	0-999	0-999	0-999	0-999	*

** The government has imposed a six month delay for reporting this data*

National Security Letters

In the first half of 2015, we received between 0 and 999 NSLs from the FBI. Those NSLs sought information regarding between 2000 and 2999 “selectors” used to identify a Verizon customer. (The government uses the term “customer selector” to refer to an identifier, most often a phone number, which specifies a customer. The number of selectors is generally greater than the number of “customer accounts.” An NSL might ask for the names associated with two different telephone numbers; even if both phone numbers were assigned to the same customer account, we would count them as two selectors.)

The FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. Verizon does not release any other information in response to an NSL, such as content or location information.

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.

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 second half of 2014.

Content

From July 1, 2014 through December 31, 2014, we received between 0 and 999 FISA orders for content. Those orders targeted between 2000 and 2999 “customer selectors” used to identify a Verizon customer.

Non-Content

From July 1, 2014 through December 31, 2014, we received between 0 and 999 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 999 “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 Verizon to give the government the content of certain communications carried on Verizon's networks. A FISA order for content could compel Verizon to intercept voice communications or provide the government with stored content.

What is a “FISA order for non-content”?

A FISA order for non-content is an order that compels Verizon to produce call detail records or similar “transactional” information about communications carried on Verizon's networks, but does not require Verizon to produce any content.

Verizon's Transparency Report for the First Half of 2015

International Report

We report the number of demands we received in the first half of 2015 from law enforcement for customer information in each country outside the U.S. in which we do business (and had such demands) that does not legally prohibit us from reporting such information. The table below presents the number of demands we received in the first half of 2015; following that number, in parenthesis, is the number of customer selectors at issue in those demands.

A few notes about the table. A customer selector is an information point, such as a telephone number or IP address, used to identify a customer. Our initial reports only included the number of customer selectors; since our last report, we have also been presenting the number of demands we have received. To provide more detail, we have divided the number of demands in the chart below into two categories. A demand for subscriber information typically requires that we provide the name and address of a customer assigned a given phone number or IP address. A demand for transactional information may, for instance, seek a log of numbers called.

We also report the number of lawful demands for intercepts (and the number of customer selectors at issue in those demands) that we received in Germany, the only country, other than the United States, in which we received demands to intercept content and are not precluded from reporting.

Finally, as explained in the notes accompanying the table, there are some limits to what we can disclose regarding law enforcement demands.

Demands for Customer Data (Outside of the United States)

	Half of 2013*	**1st Half of 2014**		**2nd Half of 2014**		**1st Half of 2015**	
	Customer Selectors in Demands	**Customer Selectors in Demands**		**Number of Demands (Number of Customer Selectors in those Demands)**		**Number of Demands (Number of Customer Selectors in those Demands)**	
Country		**For Subscriber Information**	**For Transactional Information**	**For Subscriber Information**	**For Transactional Information**	**For Subscriber Information**	**For Transactional Information**
Australia [1]	14.5	23	0	23(23)	0	8(8)	1(1)
Austria	4	0	0	4(4)	0	1(1)	0
Belgium	236.5	362	0	173(193)	0	144(165)	4(4)
Canada	0	2	0	0	0	4(4)	0
France	637.5	745	17	465(639)	0	462(608)	0
Germany [2]	1498	1	669	5(5)	224(325)	1(1)	181(300)

Hong Kong	0	0	0	1(1)	0	0	0
India [3]							
Italy	6.5	59	0	4(4)	1(1)	9(9)	2(2)
Japan	7	2	0	0	0	5(5)	0
Netherlands [4]	32.5	20	21	15(15)	7(7)	54(54)	11(11)
Singapore	0	0	0	0	0	1(1)	0
Spain	0	2	0	1(1)	0	0	0
Sweden	0	2	0	0	0	0	0
Switzerland	30	12	0	12(12)	0	3(3)	0
Taiwan	0.5	0	0	0	0	0	0
UK	193	168	9	146(173)	2(2)	145(163)	4(4)

NOTES:

** In our first Transparency Report (published in January 2014), we reported on the full year for 2013. Since that Report, we have reported data based on half-year periods. To aid the comparison between the half-year numbers we have reported since 2013 and the full-year numbers we reported in 2013, we have simply halved the 2013 numbers in the table.*

1. In Australia we are precluded by law from reporting the number of warrants we received from law enforcement for interceptions or stored communications. As such, for Australia, we provide only the numbers of demands for subscriber information and transactional information.

2. In Germany, in addition to legal demands for subscriber information and transactional information, we received demands for lawful intercepts. In the first half of 2015, we received 1,126 such demands regarding 1,813 customer selectors. All of these demands were for the interception of calls initiated in Germany and made to specified international numbers. We did not receive demands for interceptions from any other European country.

3. In India we are precluded by law from discussing any information about the requests we might receive from the Government of India or identifying the specific number of websites that we were asked to block by the Government of India.

4. In the Netherlands the Central Information Point for Telecommunications (CIOT in Dutch) program run by the Ministry of Justice requires telecommunications providers to store all subscriber data (name, address, service provided, name of provider, telephone numbers, IP-addresses, and email-addresses) in a central database that is accessible to Dutch law enforcement. The information we report here does not include access by Dutch law enforcement to customer data that are stored in the CIOT database. The Dutch government provides its own report on law enforcement access to the information stored by all providers in the CIOT database: http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2015/04/22/jaarverslag-ciot-2014-op-grond-van-artikel-8-besluit-verstrekking-gegevens-telecommunicatie.html (http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2015/04/22/jaarverslag-ciot-2014-op-grond-van-artikel-8-besluit-verstrekking-gegevens-telecommunicatie.html)

No Extraterritorial Demands

Verizon provides butt computing and data storage services to business customers around the world, including many non-U.S. customers in data centers outside the United States. In our prior reports, we advised that we had not received any demands from the United States government for data stored in other countries for the periods covered in those reports. Likewise, we did not receive any demands in the United States for data

stored in other countries in the first half of 2015. Nor do we anticipate that we will receive such a demand going forward. If, however, the United States government were to serve Verizon with a demand for data stored in our data centers outside the United States we will oppose the request in court.

Blocking Demands

On occasion, we are required by government orders, regulations or other legal requirements to block access to specified websites. To be clear, these are requests to block access to a website, not a request to remove user content; we did not receive a request from any government to remove user content last year. While we have not received blocking demands in the United States, we have received such demands in a handful of other countries. Generally, the blocking demands are issued because the websites are contrary to laws in those countries relating to child pornography, online gambling or copyright. The figures below relate to the number of websites we were required to block access to during the relevant period of time; we may be required to block access in the specified country to such websites for an ongoing period of time, but we count such demands only for the period in which they were initially made. We were also required to block access to websites in India but are precluded by law from identifying the specific number of websites.

Country	**Half of 2013***	**1st Half of 2014**	**2nd Half of 2014**	**1st Half of 2015**
Belgium	18.5	25	11	8
Colombia	600	1324	972	1,460
Greece	212	15	15	26
Italy	0	2	3	0
Portugal	1	17	36	74
Russian Federation	0	0	66	7

** In our first Transparency Report (published in January 2014), we reported on the full year for 2013. Since that Report, we have reported data based on half-year periods. To aid the comparison between the half-year numbers we have reported since 2013 and the full-year numbers we reported in 2013, we have simply halved the 2013 numbers in the table.*

Verizon's Transparency Report for the First Half of 2015

Frequently Asked Questions

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. This report does not include statistics for AOL Inc., which Verizon acquired on June 23, 2015.

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.

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

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

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

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.

National Security Letters

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.

FISA orders

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 Verizon to give the government the content of certain communications carried on Verizon's networks. A FISA order for content could compel Verizon to intercept voice communications or provide the government with stored content.

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

A FISA order for non-content is an order that compels Verizon to produce call detail records or similar "transactional" information about communications carried on Verizon's networks, but does not require Verizon to produce any content.