Verizon Transparency Report

U.S. Data

In 2013, Verizon received approximately 320,000 requests for customer information from federal, state or local law enforcement in the United States. 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 table below sets out the number of subpoenas, orders, and warrants we received from law enforcement in the United States last year. We also received emergency requests and National Security Letters. The vast majority of these various types of demands relate to our consumer customers; we receive relatively few demands regarding our enterprise customers.

Overall, we saw an increase in the number of demands we received in 2013, as compared to 2012.

Law Enforcement Demands for Customer Data — United States (2013)	
Subpoenas	164,184
Orders	70,665 62,857 General Orders 6,312 Pen Registers/ Trap & Trace Orders 1,496 Wiretap Orders
Warrants	36,696
Emergency Requests From Law Enforcement	50,000 (approximately)
Total	**321,545**
National Security Letters	**1000-1999**

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?

Like all other companies to issue transparency reports, we are not permitted at this time to report information on national security orders (like FISA orders). We do report, within a range, the number of National Security Letters that we received from the FBI in 2013; we report only a range because, like the other companies that have published transparency reports, we have not been granted permission to indicate the exact number of National Security Letters we received. Last week, President Obama announced that telecommunications providers will be permitted to make public more information in the future; we encourage greater transparency and, if permitted, will make those additional disclosures.

Does Verizon reject law enforcement demands?

Yes. If a demand is facially invalid, or if a demand seeks certain information that can only be obtained with a different form of process (for example, a subpoena, rather than a warrant, improperly is used to seek stored customer content), we reject the demand. If a demand is overly broad or vague we will not produce any information, or will seek to narrow the scope of the demand and produce a subset of the information sought. In many cases we do not produce any information at all, including because the demand seeks information we do not have.

Is Verizon reporting on the percentage of demands for which it did not produce any data?

We did not track the percentage of demands to which we produced some or no data in 2013, but will be doing so going forward. As just noted, we carefully review each demand and reject in whole or part those that are deficient.

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 approximately 164,000 subpoenas from law enforcement in the United States last year. We are required by law to provide the information requested in a valid subpoena. The subpoenas we receive are generally used by law enforcement to obtain subscriber information or the type of information that appears on a customer's phone bill. More than half of the subpoenas we receive seek only subscriber information: that is, those subpoenas typically require us to provide the name and address of a customer assigned a given phone number or IP address. Other subpoenas also ask for certain transactional information, such as phone numbers that a customer called. The types of information we can provide in response to a subpoena are limited by law. We do not release contents of communications (such as text messages or emails) or cell site location information in response to subpoenas.

Does a law enforcement officer need to go before a judge to issue a subpoena?

Under federal law and the law in many states the government does not need judicial approval to issue a subpoena. A prosecutor or law enforcement official may issue a subpoena to seek evidence relevant to the investigation of a possible crime.

Are there limits on the types of data law enforcement can obtain through a subpoena?

Yes, in response to a subpoena, we only release the six types of information specifically identified in section 2703(c)(2)(A)-(F) of Title 18 of the United States Code: customer name, address, telephone or other subscriber number, length of service, calling records and payment records. Some states have stricter rules. We do not release any content of a communication in response to a subpoena.

Are there different types of subpoenas?

Yes, we may receive three different types of subpoenas from law enforcement: a grand jury subpoena (the subpoena is issued in the name of a grand jury investigating a potential crime); an administrative subpoena (generally, a federal or state law authorizes a law enforcement agency to issue a subpoena); or a trial subpoena (the subpoena is issued in the name of the court in anticipation of a trial or hearing).

Orders

We received about 70,000 court orders last year. 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 last year – almost 63,000 – 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. Almost half of the general orders required us to release the same types of basic information that could also be released pursuant to a subpoena. We do not provide law enforcement any stored content (such as text messages or email) in response to a general order.

"Pen/Trap" Orders and Wiretap Orders. A small subset of the orders we received last year – about 7,800 – 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 about 6,300 court orders to assist with pen registers or trap and traces last 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 about 1,500 wiretap orders last year.

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 about 36,000 warrants last year. To obtain a warrant a law enforcement officer must show a judge that there is “probable cause” to believe that the evidence sought is related to a crime. This is a higher standard than the standard for a general order. While many warrants seek the same types of information that can also be obtained through a general order or subpoena, most warrants we received in 2013 sought stored content or location information.

What showing must law enforcement make to obtain a warrant?

To obtain a warrant a law enforcement officer has to show a judge that there is probable cause to believe that the evidence it seeks is related to a crime and in the specific place to be searched.

What is the difference between stored content and non-content?

“Stored content” refers to communications or other data that our users create and store through our services, such as text messages, email or photographs. We require a warrant before disclosing stored content to law enforcement, absent an emergency involving the danger of death or serious physical injury. Non-content refers to records we create such as subscriber information that a customer provides at the time she signs-up for our services, and transactional information regarding the customer’s use of our services, such as phone numbers that a customer called.

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 warrant; we do not produce stored content in response to a general order or subpoena. Last year, we received approximately 14,500 warrants for stored content.

As explained above, law enforcement may also present a wiretap order to obtain access to the content of a communication as it is taking place, which they did about 1,500 times last year. Taken together, the number of orders for stored content and to wiretap content in real-time accounted for only about five percent of the total number of demands we received in 2013.

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. Last year, we received about 35,000 demands for location data: about 24,000 of those were through orders and about 11,000 through warrants. In addition, we received about 3,200 warrants or court orders for "cell tower dumps" last 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. The number of warrants and orders for location information are increasing each 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 regarding particular 9-1-1 calls from the public. Calls for emergency services, such as police, fire or ambulance, are answered in call centers throughout the country, known as PSAPs. PSAPs receive tens of millions of calls from 9-1-1 callers each year, and certain information about the calls (name and address for wireline callers; phone numbers and available location information for wireless callers) is typically made available to the PSAP when a 9-1-1 call is made. Yet a small percentage of the time PSAP officials need to contact the telecom provider to get information that was not automatically communicated by virtue of the 9-1-1 call or by the 9-1-1 caller.

In 2013, we received 85,116 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury or from PSAPs relating to particular 9-1-1 calls from the public for emergency services. While in 2013 we did not track whether an emergency request was made by law enforcement or PSAPs, we are doing so now. We estimate that at least half of these requests – approximately 50,000 – were from law enforcement pursuant to the emergency procedures discussed above and the remainder were from PSAPs after receiving 9-1-1 calls from the public.

National Security Letters

We also received between 1,000 and 2,000 National Security Letters in 2013. We are not permitted to disclose the exact number of National Security Letters that were issued to us, but the government will allow us to provide a broad range.

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.

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

We report only information about National Security Letters. Like all other companies to issue transparency reports, we are not permitted at this time to report information on national security orders (like FISA orders).