Transparency Report FAQs
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 in June 2015; AOL is issuing its 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.

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 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.

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.