United States Transparency Report

2024 | 2nd half

verizon

Verizon's Transparency Report for the second half of 2024

Verizon's Transparency Report presents the number of demands we received from law enforcement in the United States and other countries where we did business during the second half of 2024.

United States report

The following table sets out the number of subpoenas, orders, warrants, and emergency requests that we received from federal, state, or local law enforcement in the United States during the second half of 2024. The table reports data from recent years. Data from prior periods can be found by clicking the "Archive" tab at the top of the page.

The vast majority of these 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 compared to prior six-month periods. In general, we have seen an increase in the number of warrants and a decrease in the number of general orders since 2018. (We refer to a "general order" as any order other than a pen register, trap and trace, wiretap, or warrant.) This is due in part to a Supreme Court ruling requiring law enforcement to demonstrate probable cause before obtaining location information.

Law enforcement demands for customer data – United States

	2H 2020	1H 2021	2H 2021	1H 2022	2H 2022	1H 2023	2H 2023	1H 2024	2H 2024
Subpoenas	59,264	63,665	56,641	59,456	54,681	61,919	61,120	72,856	73,862
General orders	4,062	3,841	3,485	3,809	3,400	3,539	3,549	4,362	4,532
Pen register/ trap & traces	4,492	4,242	3,830	3,961	3,970	4,393	5,137	6,108	5,999
Wiretaps	627	415	387	313	286	382	319	384	303
Warrants	15,061	15,139	14,233	16,415	17,373	21,835	21,718	25,945	25,031
Emergency requests from law enforcement	37,760	34,976	35,726	32,618	35,251	35, 698	36,033	35,540	36,564
Total	**121,266**	**122,278**	**114,302**	**116,572**	**114,961**	**127,766**	**127,876**	**145,195**	**146,291**

Verizon has teams that carefully review each demand we receive. We do not produce information in response to all demands we receive. During the second half of 2024, we did not release records in response to approximately 10% of all demands we received. Specifi ally, we did not release records in response to approximately 9% of the subpoenas we received and approximately 13% of the warrants and orders we received. We may decline to release records for a number of reasons. In some instances, including situations when a di erent type of legal process is needed for the type of information requested, the legal demand is invalid and therefore rejected. Often, we receive valid demands seeking information about a phone number serviced by a di erent provider, meaning that we have no records to produce. Likewise, we regularly receive demands seeking data that we do not possess. This includes situations where we do not collect the type of data that law enforcement seeks or where the requested data is beyond our retention periods.

We also received National Security Letters (NSLs) and Foreign Intelligence Surveillance Act (FISA) Orders, which we address in a separate table at the end of this Transparency Report.

Civil demands

Although this Transparency Report focuses on the demands we receive from law enforcement, we also receive discovery requests for data in civil cases. Our team carefully reviews each civil request to ensure its validity, just as we do in criminal cases. Subpoenas in civil cases are generally issued pursuant to authorities like Rule 45 of the Federal Rules of Civil Procedure and similar state rules. Each subpoena must seek relevant information, and that information must be shared with the other party or parties in the civil lawsuit.

During the second half of 2024, Verizon received 8,975 subpoenas in civil cases. The 8,975 civil subpoenas sought information about 19,291 customer selectors. The term “customer selector” refers to an identifier (mo t often a telephone number) that specifie a given customer. Demands often seek information about multiple selectors pertaining to the same customer. (For example, a demand may seek information on multiple phone numbers belonging to the same customer.) For this reason, the number of selectors listed in this Transparency Report is typically greater than the number of customer accounts. Approximately 60% of the civil requests we received sought information on only one selector (and thus only one customer), and over 90% sought information regarding three or fewer selectors (and thus three or fewer customers). During the second half of 2024, we did not produce any data in response to 49% of civil discovery requests. Like with criminal demands, some civil requests were legally invalid or should have been directed toward di erent providers. However, the most common reason why we did not produce records in civil cases was that responsive records were no longer available by the time when we received the request. While law enforcement demands in criminal cases typically seek relatively recent records, civil requests are often submitted long after the relevant events have occurred. As we retain customer records only for the duration necessary to meet our business needs, many civil requests seek records that have already surpassed our record retention periods.

Subpoenas

We received 73,862 subpoenas from law enforcement in the United States during the second half of 2024. We are required by law to provide the information requested by a valid subpoena. About half of the subpoenas we receive are used by law enforcement to obtain "subscriber information." Those subpoenas typically require us to provide only the name and address of the customer associated with a given phone number or IP address. Other subpoenas may ask for certain transactional information, such as the phone numbers that a customer has called. The types of information that we can provide in response to subpoenas are limited by law. We do not release the contents of communications (such as text messages or emails) or cell site location information in response to subpoenas.

During the second half of 2024, the 72,862 subpoenas we received sought information regarding 136,220 "customer selectors," which are information points (such as telephone numbers) used to identify customers. On average, each subpoena sought information about 1.8 selectors. Recall that the number of selectors is usually greater than the number of customer accounts. During the second half of 2024, approximately 73% of the subpoenas we received sought information on only one selector (and thus only one customer), and over 90% sought information regarding three or fewer selectors (and thus three or fewer customers).

Orders

A court order must be signed by a judge and must indicate that the law enforcement officer has made the oper showing required under the law. Court orders may compel us to provide certain types of information to the government. We do not provide law enforcement any content (such as text messages or emails) in response to a general order.

General orders

During the second half of 2024, we received 4,532 "general orders." We use the term "general order" to refer to any order that is not a wiretap order, pen register order, trap and trace order, or warrant. We continue to see that many of these general orders require us to release the same basic types of information that could also be released pursuant to a subpoena.

Pen/traps and wiretaps

We received 6,302 demands during the second half of 2024 that required 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 an increasing number of these requests 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 5,999 orders to assist with pen registers or trap and trace devices during the second half of 2024, although generally a single demand is issued to establish both a pen register and a trap and trace. Far less often, we are required to assist with wiretaps, where law enforcement accesses the content of a communication as it is taking place. We received 303 orders for wiretaps during the second half of 2024.

Warrants

We received 25,031 warrants during the second half of 2024. 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 legal standard than what is required 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.

During the second half of 2024, we received a total of 29,563 general orders and warrants. They sought data regarding 52,553 "customer selectors," which are information points (such as telephone numbers) used to identify customers. On average, each order or warrant sought information about 1.8 selectors. Recall that the number of selectors is usually greater than the number of customer accounts. During the second half of 2024, approximately 78% of the orders and warrants we received sought information on only one selector (and thus only one customer), and about 95% sought information regarding three or fewer selectors (and thus three or fewer customers).

Content and location information

Content

We are compelled to provide the 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 emails. 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 2024, we received 11,733 warrants for stored content.

Location information

During the second half of 2024, we received 22,486 warrants based on probable cause for location data. In addition, we received 5,725 warrants or court orders for "cell tower dumps" during the second half of 2024. In attempting 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 may request information from Verizon that is needed to help resolve serious emergencies. We are authorized by federal law to provide the requested information during such emergencies, and we have an established process for responding to these emergency requests in accordance with the law. To request data during these emergencies, a law enforcement officer must certify in writing that there is an emergency involving the danger of death or serious physical injury to a person that requires 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 submitted 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, fi e department, or ambulance, are answered in call centers (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, or phone numbers and available location information for wireless callers) is typically made available to the PSAP when a 9-1-1 call is made. Occasionally, PSAP offic ls may need to contact the relevant telecom provider to obtain information that was not automatically communicated by virtue of the 9-1-1 call or by the 9-1-1 caller.

During the second half of 2024, we received 36,564 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury. During that same period, we also received 6,982 emergency requests from PSAPs related to particular 9-1-1 calls from the public for emergency services.

National security demands

The table below sets forth the number of national security demands that we received during the applicable period. Under Section 603 of the USA FREEDOM Act, we are now able to report the number of these demands in bands of 500.

	July 1, 2020 – Dec. 31, 2020	Jan. 1, 2021 – June 30, 2021	July 1, 2021 – Dec. 31, 2021	Jan. 1, 2022 – June 30, 2022	July 1, 2022 – Dec. 31, 2022	Jan. 1, 2023 – June 30, 2023	July 1, 2023 – Dec. 31, 2023	Jan. 1, 2024 – June 30, 2024	July 1, 2024 – Dec. 31, 2024
National security letters	2-499	500-999	0-499	0-499	0-499	0-499	0-499	0-499	0-499
Number of customer selectors	1,000-1,499	1,500-1,999	1,000-1,499	1,500-1,999	1,000-1,499	1,000-1,499	1,000-1,499	1,000-1,499	1,000-1,499
FISA orders (content)	0-499	0-499	0-499	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	1,000-1,499	1,000-1,499	1,000-1,499	1,000-1,499	1,000-1,499	500-999	500-999	0-499	*
FISA orders (non-content)	0-499	0-499	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	0-499	500-999	*

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

National security letters

During the second half of 2024, we received between zero and 499 NSLs from the FBI. Those NSLs sought information regarding between 1,000 and 1,499 "customer selectors," which are information points (such as telephone numbers) used to identify customers. Recall that the number of selectors is usually greater than the number of customer accounts. 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, such as content or location information, in response to an NSL.

NSLs typically prohibit the recipient, such as Verizon, from disclosing to any other person that the NSL was received or that the recipient provided information in response to it. Until recently, these non-disclosure requirements applied indefini ely. The USA FREEDOM Act, however, requires the FBI to periodically review whether each NSL recipient could be relieved of the non-disclosure requirements. To that end, we have recently received 6 notices from the FBI advising that the non-disclosure requirements of 6 NSLs no longer apply.

We therefore can now disclose that we complied with each of those NSLs by providing the name, address, dates of service, and/or toll billing records, as authorized by the relevant statute.

Foreign Intelligence Surveillance Act orders

The government requires that we delay reporting our receipt of any orders issued under FISA for six months. Thus, at this time, the most recent FISA information that we may report is for the fir t half of 2024.

Content

From January 1, 2024 through June 30, 2024, we received between zero and 499 FISA orders for content. Those orders targeted between 500 and 999 "customer selectors" used to identify Verizon customers.

Non-content

From July 1, 2023 through December 31, 2023, we received between zero 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 counted them as FISA orders for non-content. Those orders targeted between zero and 499 "customer selectors."

Frequently asked questions

Which Verizon services does this Transparency Report cover?

The figu es in this Report include demands for customer data regarding our Verizon wireline services (such as phone, Internet, or television), our Verizon Wireless services, Visible by Verizon, our TracFone Wireless brands, and our telematics services.

Does Verizon charge law enforcement for providing data?

In some instances, federal law and most states' laws authorize providers to charge a reimbursement fee for responding to law enforcement demands for records or to recoup reasonable expenses incurred in complying with a wiretap order or pen register or trap and trace order. In most instances, however, we do not seek reimbursement for responding to law enforcement demands. 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 demands for data in civil cases?

Yes, we do. Demands in civil cases comprise a small percentage of the total requests we receive. This Transparency Report focuses on demands 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 must 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 must report to Congress each year regarding information obtained in emergencies, in some contexts. See 18 U.S.C. § 2702(d). The Director of the FBI must report twice each year to Congress regarding the number of National Security Letters issued. See 18 U.S.C. § 2709(e).

How does Verizon respect privacy and free expression when responding to law enforcement demands?

We pay careful attention to law enforcement demands to obtain customer data or to restrict access to information, and we carefully review each demand that we receive to ensure that it is valid. We seek to minimize disclosure of customer data by carefully interpreting demands and may seek clarifi ation, request modifi ation, or pursue other options, including contesting a demand, if circumstances warrant. We also seek to be accountable and transparent by sharing information about how we handle demands and about our disclosure of customer data.

Verizon is committed to operating with respect for internationally recognized human rights. For more information on Verizon's approach to human rights, see here.

Does Verizon receive demands to block content?

Although we have not received blocking demands in the United States, we have received such demands in a handful of other countries. This is detailed in our International Report. We do not receive demands from governments to remove content.

Does Verizon receive requests to shut down or restrict access to its network?

No, Verizon has not received government orders to shut down or restrict access to our services or communications networks. If we received such a request, we would evaluate its legality and proportionality and strive to minimize any impact on customers' freedom of expression and human rights. Such incidents would be disclosed in our semi-annual Transparency Report, consistent with the requirements of applicable laws.

Subpoenas

Does a law enforcement officer need to go fore 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 y issue a subpoena to seek evidence relevant to the investigation of a possible crime.

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

Yes, in response to a subpoena, we only release the six types of information specifi ally identified in 18 .S.C. § 2703(c)(2)(A)-(F): 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 di erent types of subpoenas?

Yes, we may receive three di erent 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 a ord access to "dialing, routing, addressing, or signaling information." In response to a pen register order, we must a ord real-time access to the numbers that a customer dials (or IP addresses that a customer visits). In response to a trap and trace order, we must a ord 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 di erent legal standards that law enforcement must satisfy for the di erent types of orders?

A wiretap order is the most difficult type f order for law enforcement to obtain. Under the law, law enforcement may not obtain a wiretap order unless a judge finds th t there is probable cause to believe that an individual is committing one of certain specifie o enses and that particular communications concerning that o ense will be obtained through the wiretap. A wiretap order is only issued for a specified period f time.

A general order requires law enforcement to o er specific and articulable acts 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 by demonstrating that the information likely to be obtained is relevant to an ongoing criminal investigation.

Warrants

What legal standard must law enforcement satisfy to obtain a warrant?

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

What is the di erence 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 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 customers provide when they sign up for our services. Non-content also includes transactional information regarding customers' use of our services, such as the phone numbers that a customer called.

National security letters

What is an NSL?

A National Security Letter (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 (FBI) issues an NSL to a wire or electronic communications provider (like Verizon), the 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 (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 it 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.