



Sprint Corporation

Transparency Report

Published January, 2018

This report covers information about government demands for customer information in connection with criminal and national security investigations.

The Sprint Corporation Transparency Report provides our customers and the public with information regarding Sprint's compliance with government demands for customer information. Sprint takes its obligations to safeguard our customers' privacy seriously. Protecting our customers' information is part of the understanding we have with our customers, who trust us to deliver products and services to them. From time to time, we are required, like all companies, to provide information in response to government investigations, and we ensure that all requests are valid and lawful before we comply. This report provides information about these government demands for customer information.

Sprint provides customer information to the government only in response to lawful requests or when consistent with applicable federal and state law. Requests for customer information that do not meet federal and state legal requirements are rejected.

Throughout the following pages, Sprint provides details on our compliance with lawful government demands, including search warrants, court orders, subpoenas and emergency requests, and provides the approximate numbers of such demands that the company receives or implements. Some information, as described below, is included in more than one category due to Sprint's internal tracking and due to the nature of lawful government demands. A single court order, for example, could demand customer records, location data, and the implementation of a pen register/trap and trace.

Government Requests for Customer Information

Type of Request	Number Received Between		
	July 1, 2016 to December 31, 2016	January 1, 2017 to June 30, 2017	July 1, 2017 to December 31, 2017
Subpoenas	57,627	73,462	63,166
Court Orders	14,320	15,544	14,051
Search Warrants	9,140	9,723	9,258
Emergency Requests	33,540	31,881	30,578

Types of Government Requests for Customer Information

Subpoenas:

Subpoenas typically are used to obtain information about customers, which is often referred to as “basic subscriber information.” This information is limited to the customer’s name and address, telephone connection records for the customer, information regarding length of service and types of services used, the customer’s telephone number (including temporarily assigned network addresses) and customer payment information. In most cases a subpoena requires no judicial oversight, and it may be issued directly by a law enforcement agency or government entity.

Court Orders:

The information Sprint provides to the government in response to a court order differs depending on the legal standard under which the order was obtained. For court orders that are based on a finding that the records sought are “relevant and material” to an ongoing criminal investigation, Sprint may produce any records that are requested, but not the content of communications (i.e., non-content records). This information may include incoming and outgoing telephone numbers and the locations of the cell towers used during a phone call or when sending or receiving a text message, except in those jurisdictions where a search warrant is required for this type of historical location information.

For court orders based on a finding of “probable cause,” meaning a likelihood that the request will provide evidence of a crime, Sprint may produce location information for a device in real time. In addition, court orders may compel Sprint to identify the telephone numbers for all calls that use a specific cell tower to connect to Sprint’s network during a specific period of time.

Some specific types of court orders are discussed below.

Pen Registers and Trap and Traces:

Sprint receives court orders requiring us to implement pen registers/trap and traces on behalf of law enforcement. A pen register/trap and trace allows Sprint to send dialed digits, both inbound and outbound to law enforcement. Sprint tracks the number of times we are required to implement a pen register/trap and trace on a Sprint customer's account, either by court order or in connection with an emergency request.

In order to obtain court orders for implementation of pen registers/trap and traces, law enforcement must show that the information likely to be obtained is relevant to an ongoing criminal investigation. No content (email, text messages, voicemail or pictures) is disclosed to the government in connection with a pen register/trap and trace. (In connection with pen register/ trap and trace orders, Sprint often receives so-called "secondary orders" in which law enforcement seeks information relating to the numbers that were generated by the pen register/trap and trace. The number of secondary orders is included in the total numbers of court orders described above.)

Wiretaps:

Sprint receives court orders requiring a "wiretap," or real-time access to the content of telephone or Internet communications of a Sprint customer for a limited period of time. Sprint tracks the number of times we are required to implement a wiretap on a Sprint customer account, either by court order or in connection with an emergency request.

The majority of wiretap orders compel Sprint to assist law enforcement by providing real-time voice communications of its customers. However, wiretap orders also can compel Sprint to provide text messages or Internet communications. In order for us to implement a wiretap, the court order must include a finding of probable cause that the wiretap will result in evidence of a crime and must comply with further requirements.

Real-Time Location Requests:

Sprint receives court orders requiring the provision of information regarding real-time location of a customer device on the Sprint network. Sprint tracks the number of times we are required to provide real-time location information of a Sprint customer, either by court order or in connection with an emergency request.

This table provides a summary for each of the types of requests discussed above.

Type of Request	Number Implemented Between		
	July 1, 2016 to December 31, 2016	January 1, 2017 to June 30, 2017	July 1, 2017 to December 31, 2017
Pen Register and Trap and Trace	2,799	3,036	2,949
Wiretap	1,076	1,059	1,004
Real-Time Location Requests	30,382	29,868	29,894

Search Warrants:

Search warrants are signed by a judge and, among other things, require a finding of “probable cause” that the request likely will provide evidence that a crime has been committed.

A search warrant can be used to compel Sprint to produce any non-content customer records that can be obtained with a subpoena or court order, plus any stored records containing the content of communications, such as text messages and voicemail messages. Sprint currently does not store customer text messages, email or pictures sent or received. As a result, we cannot produce this content in response to a search warrant. Search warrants also can require Sprint to produce real-time location information for a customer’s device.

Emergency Requests:

Sprint receives emergency requests for information in a number of circumstances, including requests from law enforcement agencies responding to kidnappings, violent crimes, bomb threats, search and rescue situations, and other life-threatening circumstances. Emergency requests may come from law enforcement or an emergency operator who receives a 911 call from the public. The customer information that is requested in an emergency varies and can include customer records, real-time location information or even real-time access to communications.

Even during times of emergency, Sprint has procedures in place to ensure that we release customer information only when the request meets the appropriate legal standard for the specific type of information being requested.

National Security Requests for Customer Information

Type of Request	January 1, 2016 to June 30, 2016	July 1, 2016 to December 31, 2016	January 1, 2017 to June 30, 2017
National Security Letters Received	0-999	0-999	0-999
Customer Accounts Affected by NSLs	0-999	0-999	0-999
FISA Order for Content	0-999	0-999	0-999
Customer Selectors Targeted by FISA Content Orders	2000-2999	1000-1999	2000-2999
FISA Orders for Non-Content	0-999	0-999	0-999
Customer Selectors Targeted by FISA Non-Content Orders	0-999	0-999	0-999

National Security Letters:

National Security Letters (NSLs) are requests from the Federal Bureau of Investigation (FBI) for the name, address, length of service and toll billing records of a Sprint customer for use in a national security investigation. NSLs are similar to subpoenas in that both can be issued by the investigating agency (in the case of NSLs, only by the FBI) without any court review. The legal standard required for an NSL is that the “records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.” Section 604(a) of the USA FREEDOM Act of 2015, signed by President Obama on June 2, 2015, authorize a number of options for Sprint to report the total number of NSLs received and the total number of affected customers for six-month or year-long periods, in different number ranges that begin with zero (e.g., 0-999). These options usually require that any NSL reporting incorporates a six-month delay from the date of the NSL.

Foreign Intelligence Surveillance Act Orders:

The Foreign Intelligence Surveillance Court is authorized by the Foreign Intelligence Surveillance Act of 1978 (FISA) to issue surveillance orders in connection with national security investigations. FISA provides for five types of court-ordered (or court-approved) surveillance:

- (1) Electronic surveillance (real-time content);
- (2) Physical search (stored content);

(3) Pen register and trap and trace (real-time non-content);

(4) Business records (stored non-content); and

(5) Directives (real-time and stored content and non-content relating to “non-U.S. persons” located overseas).

Section 604(a) of the USA FREEDOM Act of 2015, signed by President Obama on June 2, 2015, authorizes a number of options for Sprint to report the total number of FISAs received and the total number of affected customers for six-month or year-long periods, in different number ranges that begin with zero (e.g., 0-999). These options usually require that any FISA reporting incorporates a six-month delay from the date of the FISA.

Sprint understands the term “customer selector targeted,” which is a statutory term used in Section 604(a) of the USA FREEDOM Act of 2015, to refer to a specific identifier for an actual or potential Sprint customer (e.g., telephone number) that is identified in one of the FISA processes described above.

Additional Resources:

For information on Sprint’s commitment to transparency, please visit:

- [Our Privacy Policy](#)
- [Our Privacy and Security website](#)