



T-Mobile US, Inc. Transparency Report for 2017

This Transparency Report provides information about responses prepared during 2017 to legal demands for customer information. This Report includes, and makes no distinction between, legal demands directed at T-Mobile and MetroPCS, which are branded units of T-Mobile US, Inc. (“TMUS”). We include all the information we are legally permitted to disclose, to the extent we maintain such information.

Since our last report covering 2016, TMUS has updated the method by which it calculates the number of lawful intercept and national security intercepts provisioned. In past reports, due to technology limitations, extension orders were included in this category. An extension order requires the carrier to continue an existing intercept for a specified duration. Advancements in technology have enabled TMUS to report this data in a more detailed manner. Accordingly, in this Report, the Pen Register/Trap and Trace, Wiretap and National Security FISA categories set forth the numbers of initial intercepts provisioned.

In addition, due to the technology advancements mentioned above, TMUS is able to provide more detailed reporting on the reasons it rejects, provides no response or otherwise is unable to respond to certain requests it receives.

How We Operate

TMUS takes very seriously the privacy of its customers’ information and its obligation to protect it from unlawful release. TMUS maintains a dedicated law enforcement relations team (referred to as “LER”), which is available 24/7/365 to handle requests from government entities and other requestors. TMUS releases customer information only when legally permitted or required.

Legal Process Required

Various federal and state statutes permit or require release of subscriber information to government entities, criminal defendants and civil litigants who issue or obtain legal demands. The legal demands can take various forms, depending on the information sought. The most common forms are subpoenas, court orders, warrants, national security letters and requests under emergency circumstances. Each type of demand has its own corresponding legal standard and requirements that the requestor must meet for the demand to be lawful. Generally speaking, the more sensitive the type of information sought, the higher the legal standard to obtain it.

The table below identifies the most common types of subscriber information requested from TMUS and type of legal process required.

Types of Information Requested	Minimum Required Legal Process	Legal Standard (Generally)
Subscriber Information (e.g., information a customer provides when signing up for service, such as name and address)	Subpoena	Based on determination that the information sought is relevant to a criminal or civil matter
Historical Transaction Detail Information (e.g., non-content information about past voice calls, text messages or data sessions, such as start time, duration, numbers called or texted)	Subpoena	Based on determination that the information sought is relevant to a criminal or civil matter
Emergency Information (e.g., subscriber information, location information, transactional detail, content (if available), in emergencies)	Certification of Emergency from Law Enforcement/Public Safety Answering Points	Good faith belief by the carrier of that an emergency exists
Real Time (prospective) Call Detail Information, Non-content (Pen register/trap and trace) (e.g., information on incoming and outgoing phone numbers for a specific phone/mobile device, time transmitted, duration of the call)	Pen Register Court Order	Relevant and material to an ongoing criminal investigation
Historical Cell Site Location Information “CSLI” (e.g., location of towers that a phone/mobile device used in the past over a specific period of time)	Court Order or Warrant*	Relevant and material to an ongoing criminal investigation or probable cause, depending on the jurisdiction*
Real Time (prospective) Audio content (e.g., phone conversation)	Wiretap Court Order	Probable cause, reasonable grounds to suspect that a crime has been committed. Only for certain serious crimes
Real Time (prospective) Content (e.g., text messages or streamed data)	Wiretap Court Order	Probable cause, reasonable grounds to suspect that a crime has been committed. Only for certain serious crimes
Real Time Location (e.g., approximate location of a phone/mobile device)	Search Warrant	Probable cause, reasonable grounds to suspect that a crime has been committed
Historical Cell Tower Dump Information (e.g., list of phone numbers which used a specific cell tower during a specific period of time)	Court Order or Search Warrant	Relevant and material to an ongoing criminal investigation or probable cause, reasonable grounds to suspect that a crime has been committed.
Stored Content (e.g., saved voicemail message)	Search Warrant	Probable cause, reasonable grounds to suspect that a crime has been committed

* In 2017, jurisdictions were split on the appropriate standard for release of CSLI. T-Mobile adhered to the standard adopted by the state in which the court issuing the legal demand was located. The recent Supreme Court decision in Carpenter v U.S. became effective in 2018, and therefore did not affect requests for CSLI during this reporting period.

In some cases, more than one form of legal process may be acceptable. For example, Subscriber Information may be obtained through a subpoena, but may also be obtained through a court order or even a warrant.

Types of Legal Demands

Below is a general description of the types of legal demands we receive.

Subpoenas

Subpoenas may be issued by government or non-government entities. Criminal defense and civil litigants are examples of non-government entities that may issue subpoenas. The subpoenas received generally request the type of information that appears on a customer's phone bill. TMUS will only release the six types of subscriber information allowed by 18 USC § 2703 pursuant to a subpoena: 1) customer name; 2) address; 3) network transactions, such as call details; 4) length of service; 5) telephone or device number or other subscriber number or identity and 6) means and source of payment information. TMUS does not release the content of a communication or information other than that included in the above listings in response to a government subpoena.

Court Orders (General)

General court orders are available to government and non-government entities. Criminal defense and civil litigants are examples of non-government entities that may request court orders. There are many different types of court orders that compel disclosure of customer information. The type of information sought determines the specific legal standard of proof that the requestor must meet. Most of the court orders received by TMUS seek subscriber information, which can also be obtained through a subpoena. A judge must review a requestor's application for a court order and will issue the order only if the requestor has made the requisite showing under the law.

Wiretap Court Orders

Wiretap court orders are available only to government entities. Court orders for wiretaps seek the content of communications in real time. A judge must review the application for any real-time monitoring and sign a court order indicating that the government has made the requisite showing under the law.

Pen Register/Trap and Trace Court Orders

Pen register/trap and trace court orders are available only to government entities. Court orders for pen registers/trap and trace seek real time non-content information on incoming and outgoing phone numbers. A judge must review the application for any real-time monitoring and

sign a court order indicating that the government has made the requisite showing under the law.

Search Warrants

Search warrants are available only to government entities. Search warrants may request the same types of information that could be obtained through a court order or even a subpoena. However, most of the warrants we receive also request historic location information or content, such as stored voicemail messages. Warrants require a showing of probable cause that a crime has been or is being committed and evidence of it will be obtained from the subscriber information sought. A judge must review the application for a search warrant and will issue the warrant only if the government has made the requisite showing under the law.

Emergency Requests

Law enforcement agencies may request information that is needed to respond to emergencies such as kidnappings, hostage situations and suicide threats. TMUS is authorized by law to provide the requested information upon law enforcement's certification that such an emergency exists. The certification must be sufficient for TMUS to form a good faith belief that there is an emergency involving danger of death or serious physical injury to any person that requires disclosure without delay of transactional records and communications relating to the emergency.

Public Safety Answering Points (PSAPs) may also request release of subscriber information when needed to respond to 9-1-1 calls from the public.

National Security Letters

The Director and certain other designated officials of the Federal Bureau of Investigation ("FBI") may issue a National Security Letter ("NSL") requesting information in national security matters. The FBI must certify in writing to the recipient of the letter that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. An NSL may request only limited information: name, address, length of service and local and long distance toll billing records.

Foreign Intelligence Surveillance Act ("FISA") Orders

The FISA Court is a special court that reviews requests for surveillance in national security cases. FISA orders require providers to facilitate electronic surveillance of an individual's activities via wiretap and/or pen register/trap and trace.

Requests from Foreign Governments

TMUS does not respond to requests from foreign entities without the express written consent of the United States Department of Justice or an order from the United States District Court. Such orders must meet the requirements of US law and the law of the jurisdiction making the request.

Summary of Types and Number of Requests in 2017

Legal Demands

The table below shows the type and the number of legal demands for which TMUS provided a response in 2017.

Type of Request (excluding National Security Requests)	Number of Requests
Subpoenas (criminal, civil and trial)	219,377
Emergency/911 Requests	140,245
Court Orders (excluding orders for wiretaps, pen register/trap and trace)	55,372
Warrants/Search Warrants	27,203
Other*	7,798
Pen Register/Trap and Trace Orders	13,020
Wiretap Orders	2,968
Customer Requests for their own information	537
Requests from Foreign Entities †	20
TOTAL	466,540

* This may include requests to preserve information pursuant to 18 USC § 2704, requests for T-Mobile information (not customer information), requests pursuant to The Fair and Accurate Credit Transactions Act of 2003, and any other request that does not match a category above.

† Australia (2), Canada (10-), Estonia (1), Germany (2), Honduras (1), Italy (1), Spain (1), Tribal Nations (2)

Rejected/No Response/Unable to Respond

The table below shows the number of legal demands that 1) were rejected, 2) received no response at all, and 3) received a written explanation regarding why T-Mobile was unable to respond in whole or in part.

Description	Number of Responses
Rejected	4,625
No Response	50,121
Unable to Respond	24,354
TOTAL	79,100

Rejections - TMUS will transmit a written rejection when it is unable to read or receives an incomplete legal demand.

No Response - TMUS will not transmit any written response when a response is not legally required.

Unable to Respond - TMUS will transmit a written "Unable to Respond" notice when it receives a legal demand that it cannot lawfully fulfill or when it does not possess/control the information sought.

Requests for Location Information

The table below shows the number of responses to legal demands for location information.

Description	Number of Requests
Requests for Historical Call Details with Cell Site Information (CSLI)	64,266
Requests for Prospective Location	46,395
Requests for Tower Dump	4855

TMUS will release historical and prospective location information upon receipt of an appropriate legal demand. (See chart, Page 2). The data above reflects the number of demands that were processed in 2017 based on a warrant or court order (depending on the type of information sought) or when a government entity requested same in connection with an emergency request. This data is a subset of the number of court orders and warrants listed above. (See chart, Page 5). PSAP requests for current location information (i.e. one-time pings) based on emergency calls to 911 are not included in the data above

Historical cell site location information (“CSLI”) details the location of the cell tower(s) which carried a particular call or other network transaction. As set forth above, in 2017, CSLI was released to the government only after receipt of a court order or a warrant, depending on the jurisdiction. CSLI may also be released to a non-government requestor upon receipt of a subpoena or when a government entity seeks same in connection with an emergency request. The Supreme Court decision in Carpenter v U.S. handed down in 2018 did not affect requests for CSLI during this reporting period.

Prospective location information consists of live location information, delivered as longitude and latitude coordinates to a government requestor. It is often referred to as geolocation or real-time GPS data. As set forth above, prospective location information is released only after receipt of a search warrant or when a government entity seeks same in connection with an emergency request.

Tower dump orders seek information regarding all subscribers and/or roamers whose network transactions are carried by a certain tower or geographic area within a delineated period of time. TMUS requires a court order or search warrant before it will release tower dump information to the government.

National Security Requests

The table below sets forth national security requests (National Security Letters and FISA Orders) we received. The USA Freedom Act of 2015, permits reporting of this information in half year increments, in bands of 500. These requests are not included in any of the above charts.

National Security Requests	Number of Requests in bands
National Security Letters 1 st half of 2017	0 – 499
National Security Letters 2 nd half of 2017	0 – 499
FISA Orders 1 st half of 2017	0 – 499
FISA Orders 2 nd half of 2017	0 – 499

Cost Recovery and Charges

Federal law permits carriers to be reimbursed for the reasonable costs of providing technical assistance for lawful surveillance activities and for costs incurred in providing stored electronic communications or backup copies to the government.

Generally, TMUS does not charge the government for the costs incurred in responding to court orders, subpoenas or emergency requests. 18 USC § 2706 precludes cost recovery relating to the release of certain subscriber information, except in cases of undue burden.

More Information

For more information regarding how we collect, use, disclose and store customer information please see our privacy policies at:

<http://www.t-mobile.com/company/website/privacypolicy.aspx>