



## T-Mobile Transparency Report for 2013 and 2014

This Transparency Report provides information about requests from law enforcement agencies and others for customer information we<sup>1</sup> received in 2013 and 2014 and describes how we respond to those requests. We include all the information we are legally permitted to disclose, to the extent we maintain such information.

We take very seriously the privacy of our customers' information and our obligation to protect it. When we receive a request from law enforcement for customer information we confirm that the request is valid and that our response complies with the law and our own policies. When a lawful request for customer information is presented to us we are required to comply. We discuss the types of law enforcement requests we receive below.

### Summary of Types of Information Requested and Legal Process

Law enforcement and government<sup>2</sup> requests can take various forms, depending on the information sought. The most common forms include subpoenas, court orders, warrants, national security letters and requests under emergency circumstances. Each type of request has its own legal standard and requirements the government must follow for the request to be lawful. Generally speaking, the more sensitive the type of information sought, the higher the legal standard to obtain it.

With respect to any type of request, T-Mobile provides customer information to law enforcement agencies only where legally permitted or required to do so. We maintain a dedicated law enforcement relations team (referred to as "LER"), which is available 24/7/365 to handle requests from law enforcement and other governmental agencies. We require law enforcement agencies to follow established legal processes when they make a request for customer information, and we examine each such request to ensure it meets all applicable legal requirements. We seek clarification if a request appears overbroad, unauthorized or omits information. If a request is beyond the scope of the law, asks for information outside of T-Mobile's control, is defective on its face or otherwise has a legal deficiency, it is rejected.

The following table provides examples of the most common types of information requested by the government and type of legal process required:

---

<sup>1</sup> T-Mobile and MetroPCS merged in 2013. The report covers both companies.

<sup>2</sup> "Government" refers primarily to "law enforcement agencies." The two terms are used interchangeably in this report.

<b>Information Type Requested</b>	<b>Minimum Required Legal Process</b>
<b>Subscriber Information</b> (e.g., information a customer provides when signing up for service, such as name and address, and call detail information)	Subpoena
<b>Historical Call Detail Information</b> (e.g., information about calls made in the past, such as start time, duration, numbers called)	Subpoena
<b>Emergency Information</b> (e.g., location information, call detail, content, in emergencies)	Certification from Law Enforcement/Public Safety Answering Points
<b>Real Time Call Detail Information</b> (e.g., information on incoming and outgoing phone numbers for a specific phone/mobile device)	Pen Register Court Order
<b>Historical Cell Site Location Information</b> (e.g., location of towers that a phone/mobile device used in the past over a specific period of time)	Court Order or Warrant*
<b>Real Time Audio</b> (e.g., phone conversation)	Wiretap Court Order
<b>Real Time Content</b> (e.g., text messages)	Wiretap Court Order
<b>Real Time Location</b> (e.g., approximate location of a phone/mobile device)	Warrant
<b>Historical Cell Tower Dump Information</b> (e.g., list of phone numbers which used a specific tower during a specific period of time)	Warrant
<b>Stored Content</b> (e.g., saved voicemail message)	Warrant

\* Depends on the applicable jurisdiction.

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.

### **Subpoenas**

Law enforcement agencies and most administrative agencies issue subpoenas to obtain information relevant to the investigation or prosecution of a crime. Subpoenas may also be issued by attorneys in criminal defense and civil litigation cases. The subpoenas we receive from law enforcement generally request the type of information that appears on a customer's phone bill. We only release the six types of subscriber information allowed by 18 USC § 2703:

1) customer name; 2) address; 3) length of service; 4) subscriber account identifiers (such as telephone number or device information); 5) network transaction records (such as call details) and 6) payment information. We do not release content of a communication or information other than that listed above in response to a government subpoena.

### **Court Orders**

There are various types of court orders that compel disclosure of customer information. The type of information sought determines the specific legal standard of proof that the government must meet. Most of the court orders we receive are for subscriber information, which can also be obtained through a subpoena. We also receive court orders for wiretaps, under which we are required to provide the content of communications in real time or in other words, as the communication is taking place. Additionally, we receive orders for pen registers/trap and trace, under which we provide real time information on incoming and outgoing phone numbers. A judge must review law enforcement's application for any real time monitoring and sign a court order indicating that the law enforcement officer has made the requisite showing under the law.

### **Warrants**

Warrants or search warrants require a showing of probable cause to believe a crime has been or is being committed and evidence of it will be obtained from the account. Warrants may sometimes request the same types of information that could be obtained through a court order or even a subpoena, but most of the warrants we receive request real-time location information or content, such as text messages and stored voicemail messages.

### **Emergency Requests**

Law enforcement may request information that is needed to respond to emergencies such as kidnappings, hostage situations and suicide threats. We are authorized by law to provide the requested information upon law enforcement's certification. The certification must be sufficient for us 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.

We may also receive emergency requests for information from Public Safety Answering Points (PSAPs) that receive 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. An NSL cannot be used to obtain anything else from T-Mobile.

## Foreign Intelligence Surveillance Act (“FISA”) Orders

The FISA Court (“FISC”) is a special court that reviews requests for surveillance in national security cases. Its orders require providers to facilitate electronic surveillance of an individual’s activities via such methods as wiretaps and pen registers.

## Requests from Foreign Governments

We do not receive many requests from foreign governments but when we do, we notify the Department of Justice, the Federal Bureau of Investigation and the Department of Homeland Security of such request as required by the terms of an agreement entered into in 2001, as amended, between these agencies, T-Mobile and Deutsche Telekom, as a condition to Deutsche Telekom acquiring ownership of T-Mobile. Only upon express written consent of the Department of Justice or a US court of competent jurisdiction, and if the request otherwise meets the requirements of US law and the law of the jurisdiction making the request, may T-Mobile respond to the foreign request.

## Summary of Types and Number of Requests

### 2014

In 2014, T-Mobile received approximately 351,940 requests for customer information and sometimes T-Mobile information (for example, information about our network). This number represents an approximate 10.8% increase compared to 2013. Approximately 3.6% of the requests were from third parties in connection with civil matters (insurance claims, divorce and personal injury cases, for example). The remainder was from federal, state or local law enforcement.

The table below provides the types of requests we receive and the approximate number of such requests:

Type of Request	Number of Requests
Subpoenas (criminal and civil)	177,549
Emergency Requests/911 calls	97,440
Court Orders (excluding orders for wiretaps, pen register/trap and trace)	34,913
Warrants/Search Warrants	17,316
Other*	8,760
Pen Register/Trap and Trace Orders	9,916
Wiretap Orders	3,087
Customer Requests for their own information	849
National Security Requests (NSLs and Foreign Intelligence Surveillance Orders Combined)**	2000 - 2250
Requests from Foreign Governments †	8

\* 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.

\*\* Providers are authorized by statute to report the national security requests in one of three ways. T-Mobile has chosen to report a combined total of national security requests for this reporting period, and may be able to report more granular information in the future. To the extent we are permitted to report this information in the aggregate, it must be in bands of 250 increments.

† Germany (1), Canada (4), Australia (1), Hong Kong (1) and Columbia (1)

## 2013

In 2013, T-Mobile received approximately 317,000 requests for customer information and sometimes T-Mobile information (for example, network information). This number represents an approximate 7% increase compared to 2012. Approximately 3% of the requests were from third parties in connection with civil matters (insurance claims, divorce and personal injury cases, for example). The remainder was from federal, state or local law enforcement.

The table below provides the types of requests we receive and the approximate number of such requests:

Type of Request	Number of Requests
Subpoenas (criminal and civil)	153,177
Emergency Requests/911 calls	93,032
Court Orders (excluding orders for wiretaps, pen register/trap and trace)	33,106
Warrants/Search Warrants	11,879
Other*	11,105
Pen Register/Trap and Trace Orders	8,595
Wiretap Orders	2,308
Customer Requests for their own information	1,724
National Security Requests (NSLs and Foreign Intelligence Surveillance Orders combined)**	2000 - 2250
Requests from Foreign Governments†	5

\* 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.

\*\* Providers are authorized by statute to report the national security requests in one of three ways. T-Mobile has chosen to report a combined total of national security requests for this reporting period, and may be able to report more granular information in the future. To the extent we are permitted to report this information in the aggregate, it must be in bands of 250 increments.

† Brazil (1), Canada (2) and Australia (2)

The average law enforcement request in both 2013 and 2014 (not including national security requests) asks for approximately fifty-five days of records for two phone numbers.

## Cost Recovery and Charges

Federal law provides that carriers are entitled to be compensated 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, T-Mobile does not charge law enforcement agencies for the costs incurred in responding to emergency requests. 18 USC § 2706 precludes us from cost recovery for producing toll records and 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>