T-Mobile Transparency Report for 2015

This Transparency Report provides information about requests we received in 2015 from law enforcement agencies and others for customer information. We include all the information we are legally permitted to disclose, to the extent we maintain such information.

Since our last report covering 2013 and 2014 we have made a number of system enhancements which allow us to provide more information on the requests we receive, for example, the number of requests we reject. Further, we discuss in greater depth the legal processes and other matters we know are of interest.

How We Operate

We take very seriously the privacy of our customers' information and our obligation to protect it. 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. 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. When a lawful request for customer information is presented to us we are required to comply. When we receive a request from law enforcement for customer information we first confirm that the request is legally valid. We seek clarification if a request is overbroad or vague or omits required 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.

What Law Enforcement Wants/Legal Process Required

A variety of laws permit or require government agencies to investigate suspected criminal activity and other wrongdoing. We receive requests for customer information from those government agencies. Law enforcement and government requests 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 request has its own corresponding legal standard and requirements that the government must meet for the request to be lawful. Generally speaking, the more sensitive the type of information sought, the higher the legal standard to obtain it.

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

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 investigation
Historical Call Detail Information (e.g., non-content information about calls or text messages made in the past, such as start time, duration, numbers called)	Subpoena	Based on determination that the information sought is relevant to a criminal investigation
Emergency Information (e.g., location information, call detail, content, in emergencies)	Certification from Law Enforcement/Public Safety Answering Points	Good faith belief by the carrier of an emergency
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 investigation
Historical Cell Site Location Information (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
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)	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 tower during a specific period of time)	Search Warrant	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

* 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.

ECPA--Content vs Non-Content

The federal law that deals with law enforcement's ability to obtain customer information is the Electronic Communications Privacy Act, known as ECPA. ECPA allows the government to obtain content as well as non-content. By way of example, content is an actual audio conversation, or a text message. Non-content would be customer name and address, or numbers dialed, for example. These distinctions are important because they will determine the type of legal demand that is required under ECPA.

TYPES of LEGAL DEMANDS

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

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 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. We do 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)

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.

Wiretap Court Orders
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.

Pen Register/Trap and Trace Court Orders
Additionally, we receive court orders for pen registers/trap and trace, under which we provide real time non-content 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.

Search 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 customer's 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. A NSL may request only limited information: name, address, length of service and local and long distance toll billing records. A NSL cannot be used to obtain anything else from T-Mobile, such as content or location information.

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/trap and trace.

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 T-Mobile, these agencies 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 in 2015

The table below shows the types of requests T-Mobile received and the approximate number of such requests we responded to in 2015:

Type of Request (excluding National Security Requests)	Number of Requests
Subpoenas (criminal and civil)	175,823
Emergency Requests/911 calls	104,506
Court Orders (excluding orders for wiretaps, pen register/trap and trace)	47,998
Warrants/Search Warrants	17,424
Other*	5,809
Pen Register/Trap and Trace Orders	16,231
Wiretap Orders	4,454
Customer Requests for their own information	211
Requests from Foreign Governments †	5
TOTAL	372,461

In addition to the above, we received approximately 70,000 requests that we rejected and did not respond to for various reasons. For example, legal demands that were for other carriers or were facially invalid.

* 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.

† Sweden (1), Japan (1) Hong Kong (1), Canada (1) Netherlands (1)

National Security Requests

The table below sets for the national security requests (National Security Letters and FISA Orders) we received. Under the USA Freedom Act of 2015, we are able to report the numbers of national security requests in one of four ways. We have chosen to report separately on these requests in half year increments, which requires reporting in bands

of 500. These requests are not included in the chart above.

National Security Requests	Number of Requests in bands
National Security Letters 1st half of 2015	0-499
National Security Letters 2nd half of 2015	0-499
FISA Orders 1st half of 2105	0-499
FISA Orders 2nd half of 2015	0-499

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