AT&T February 2018

Transparency Report

Introduction

At AT&T, we take our responsibility to protect your information and privacy very seriously. We continue our pledge to protect your privacy to the fullest extent possible and in compliance with applicable law.

Like all companies, we are required by law to provide information to government and law enforcement entities, as well as parties to civil lawsuits, by complying with court orders, subpoenas, lawful discovery requests and other legal requirements. We ensure that these requests are valid and that our responses comply with the law and our own policies.

This Report

This AT&T Transparency Report provides specific data regarding the number and types of legal demands to which we responded for the second half of 2017, as well as Foreign Intelligence Surveillance Act demands for the first half of 2017. For comparison purposes, we have included data from our prior report.

National Security Demands

National Security Letters	***Jan.–June 2017***	***July–Dec. 2017***
Total Received	500–999	500-999
Customer Selectors Targeted	3,000–3,499	3,500-3,999

Foreign Intelligence Surveillance Act	***July–Dec. 2016***	***Jan.–June 2017***
Total Content	**0–499**	**0-499**
Customer Selectors Targeted	7,500–7,999	12,500-12,999
Total Non-Content	**0–499**	**0-499**
Customer Selectors Targeted	0–499	0-499

Total U.S. Criminal & Civil Demands

Total Demands	***Jan.–June 2017***	***July–Dec. 2017***
(Federal, State and Local; Criminal and Civil)	**131,935**	**119,246**
Subpoenas	100,829	90,909
Criminal	90,445	81,169
Civil	10,384	9,740
Court Orders (General)	12,011	10,504
Historic	8,838	7,547
Real-Time (Pen registers)	3,173	2,957
Search Warrants/Probable Cause Court Orders		
Historic	12,737	11,656
Stored Content	3,912	3,662
Other	8,825	7,994
Real-Time	6,358	6,177
Wiretaps	1,219	1,127
Mobile Locate Demands	5,139	5,050

Demands Rejected/Partial or No Data Provided

(Breakout detail of data included in Total U.S. Criminal & Civil Demands)

	Jan.–June 2017	*July–Dec. 2017*
Total	**35,215**	**40,509**
Rejected/Challenged	3,910	3,350
Partial or No Information	31,305	37,159

Location Demands

(Breakout detail of data included in Total U.S. Criminal & Civil Demands)

	Jan.–June 2017	*July–Dec. 2017*
Total	**36,133**	**37,670**
Historic	26,941	29,022
Real-Time	8,299	7,729
Cell Tower	893	919

Emergency Requests

	Jan.–June 2017	*July–Dec. 2017*
Total	**55,860**	**59,838**
911	41,755	47,230
Exigent	14,105	12,608

In-Depth Analysis

National Security Demands

National Security Letters (NSL) are administrative subpoenas issued by the U.S. Federal Bureau of Investigation to compel production of information in regard to counterterrorism or counterintelligence investigations. NSLs are limited to non-content information, such as a list of phone numbers dialed or subscriber information. Legal demands issued pursuant to the Foreign Intelligence Surveillance Act (FISA) may direct us to provide content and non-content data related to national security investigations, such as international terrorism or espionage.

Our reporting on NSLs and FISA orders (collectively referred to as "National Security Demands") is governed by U.S. law.[1] By statute, we are permitted to report data of demands served on us and the "customer selectors targeted" by those respective demands in specifically defined numeric ranges and for only certain time periods.

Total U.S. Criminal & Civil Demands

This number includes demands to which we responded in connection with criminal and civil litigation matters. This category doesn't include demands reported in our National Security Demands table.

Criminal proceedings include actions by government entities — whether at the federal, state or local level — against an individual arising from an alleged violation of criminal law. Because federal, state and local investigating authorities in the U.S. may each initiate criminal proceedings, we receive demands from thousands of different law enforcement entities.

Civil actions include lawsuits involving private parties (e.g., a personal liability case, divorce proceeding or disputes between private companies or individuals). In addition, civil proceedings include investigations by governmental regulatory agencies such as the Securities and Exchange Commission, the Federal Trade Commission and the Federal Communications Commission.

Our Process

We receive multiple types of legal demands, including subpoenas, court orders and search warrants. Before we respond to **any** legal demand, we determine that we have received the correct type of demand based on the applicable law for the type of information sought. For instance, in some states we must supply call detail records if we receive a subpoena. In other states, call detail records require a probable cause court order or search warrant. If the requesting agency has failed to send the correct type of demand, we reject the demand.

[1] See 50 U.S.C. § 1874, as added by the USA Freedom Act (Public Law 114-23 of June 2, 2015).

Types of Legal Demands

The reporting category "Total U.S. Criminal & Civil Demands" reflects the type of demand with the information requested, particularly relating to General Court Orders and search warrants.

Subpoenas don't usually require the approval of a judge and are issued by an officer of the court, e.g., an attorney. They are used in both criminal and civil cases, typically to demand testimony or written business documents, such as calling records, and basic subscriber information, such as the name and address listed on the billing account.

General Court Orders are signed by a judge. We consider "general" court orders to be all orders except those that contain a probable cause finding. In a criminal case, for example, a judge may issue a court order on a lesser standard than probable cause, such as "relevant to an ongoing criminal investigation." In criminal cases, court orders are also used to demand real-time, pen register/"trap and trace" information, which provides phone numbers and other dialed information for all calls as they are made or received from the device identified in the order. In a civil case, a court order may be issued on a "relevant" or "reasonably calculated to lead to the discovery of admissible evidence" standard.

In both the criminal and civil context, general court orders have been used to demand historic information, like billing records or records relating to usage of a wireless device.

Search Warrants and Probable Cause Court Orders are signed by a judge, and they are issued only upon a finding of "probable cause." To be issued, the warrant or order must be supported by sworn testimony and sufficient evidence to believe the information demanded is evidence of a crime. Probable cause is viewed as the highest standard to demand evidence. Except in emergency circumstances, a search warrant or probable cause court order is required for all real-time precise location information (like GPS) and real-time content (such as content obtained through wiretaps). Stored content (like stored text and voice messages) generally also requires a warrant.

Foreign-Originated Demands for Information about a U.S. Consumer or Business

If we receive an international demand for information about a U.S. customer, whether an individual or business, we refer the requester to that country's Mutual Legal Assistance Treaty (MLAT) process. We did not receive any international demands for information about a U.S. customer from a country that does not have an MLAT process. The FBI ensures that we receive the proper form of U.S. process (e.g., subpoena, court order or search warrant), subject to the limitations placed on discovery in the U.S., and that cross-border data flows are handled appropriately. Thus, any international originated demands that follow an MLAT procedure are reported in our Total Demands category because we can't separate them from any other FBI legal demand we may receive.

Demand Rejected/Partial Or No Data Provided

We ensure that we receive the appropriate type of demand for the information requested. In this category, we include the number of times we rejected a demand or provided only partial information or no information in response to a demand. Here are a few reasons why certain demands fall into this category:

- The wrong type of demand is submitted by law enforcement. For instance, we will reject a subpoena demanding a wiretap, because either a probable cause court order or search warrant is required.
- The demand has errors, such as missing pages or signatures.
- The demand was not correctly addressed to AT&T.
- The demand did not contain all of the elements necessary for a response.
- We had no information that matched the customer or equipment information provided in the demand.

Location Demands

Our "Location Demands" category breaks out the number of civil and criminal legal demands we received by the type of location information (historic or real-time) demanded. Demands for location information seek precise GPS coordinates of the device or call detail records that reflect the location of any cell site processing a call. We also get demands for cell tower searches, which ask us to provide all telephone numbers registered on a particular cell tower for a certain period of time. We do not keep track of the number of telephone numbers provided to law enforcement in connection with cell tower searches.

A single cell tower demand may cover multiple towers. We disclose both the total number of demands and the total number of cell tower searches. For instance, if we received one court order that included two cell towers, we count that as one demand for two searches. For the 919 cell tower demands during this reporting period, we performed 2,624 searches. The average time period that law enforcement demanded for a cell tower search was 2 hours and 30 minutes for this reporting period.

Except in emergency situations, we require the most stringent legal standard — a search warrant or probable cause court order — for all demands for real-time precise location information. The standards vary for other types of location demands, including those for non-precise location information and historic location information. In those cases, we require a general court order, search warrant or probable cause court order, depending on the applicable state and federal laws.

Emergency Requests

The numbers provided in this category are the total of 911-originated inquiries and exigent requests that we processed during this reporting period. 911-originated inquiries are those that help locate or identify a person in need of emergency assistance. "Exigent requests" are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies. In order to protect your privacy, we require a certification from a law enforcement agency confirming they are dealing with a case involving risk of death or serious injury before we will share information sought by an exigent request.

International Demands

The "International Demands" category represents the number of civil and criminal legal demands originating outside the U.S. and related to AT&T's operations in foreign countries. These demands are for (i) historic subscriber information about consumers who reside in other countries and businesses that operate in other countries; and (ii) URL/IP (website/Internet address) blocking demands from foreign governments.

The Diverse Services AT&T Provides Internationally Affect the Types and Volume of Demands We Receive

Business Services: AT&T provides telecommunications and IT services to the foreign offices of large multi-national business customers. In all foreign countries where AT&T supports these customers, AT&T primarily receives demands for historic subscriber information. In those countries where AT&T also provides internet access service, it may also have received demands for IP or URL blocking.

Consumer Mobility Services: Mexico is the only country outside of the U.S. where AT&T provides consumer mobility service. Accordingly, AT&T received legal demands similar to those it receives in the U.S., including demands for subscriber information, location information and real-time content.

DIRECTV: In all Latin American countries where AT&T provides DIRECTV consumer satellite television service we primarily receive demands for subscriber information. In those Latin American countries where DIRECTV also provides broadband service, we also received demands for IP or URL blocking.

A Few Additional Points

- Historic Subscriber Information is information such as the name and address listed on the billing account or the types of services purchased from AT&T.
- The IP or URL blocking demands come from countries that require us to block access to websites that they deem offensive, illegal, unauthorized or otherwise inappropriate. These demands are listed separately from the demands for historic subscriber information.
- While AT&T may provide internet access in some foreign countries, we do not have the ability to control the content of any websites other than AT&T's own sites. Accordingly, while we did receive and comply with demands from foreign governments to block access to websites in their countries during this reporting period, we did not receive demands to remove content from websites (nor would we be able to do so). During this reporting period, we did not receive any demands from any foreign governments to produce any stored content.
- Finally, the laws governing the international demands that we receive differ by country. We respond to these demands based on each country's laws.[2]

[2] India, for example, does not permit publication of demands.

International Demands[3]

Total International Demands	*Jan.–June 2017*	*July–Dec. 2017*
Argentina		
Historic: Subscriber Information	657	700
IP/URL Blocking	1	0
Belgium		
Historic: Subscriber Information	0	0
IP/URL Blocking	5	3
Brazil		
Historic: Subscriber Information	234	339
IP/URL Blocking	2	1
Chile		
Historic: Subscriber Information	3	7
IP/URL Blocking	0	0
Colombia		
Historic: Subscriber Information	1,255	1,106
IP/URL Blocking	2	1
Ecuador		
Historic: Subscriber Information	95	77
IP/URL Blocking	0	0
Germany		
Historic: Subscriber Information	0	1
IP/URL Blocking	0	0
Peru		
Historic: Subscriber Information	0	12
IP/URL Blocking	0	0
Romania		
Historic: Subscriber Information	0	0
IP/URL Blocking	2	0
Russia		
Historic: Subscriber Information	0	0
IP/URL Blocking	181	180
Slovakia		
Historic: Subscriber Information	0	0
IP/URL Blocking	0	3

[3] Countries where "0" has been reported for two consecutive reporting periods (12 months) have been removed from this chart. We will add countries back in future reports should we get new requests in any of those countries.

Spain		
Historic: Subscriber Information	0	2
IP/URL Blocking	0	0
Turkey		
Historic: Subscriber Information	0	0
IP/URL Blocking	10,556	7,969
United Kingdom		
Historic: Subscriber Information	0	5
IP/URL Blocking	0	0
Uruguay		
Historic: Subscriber Information	1	2
IP/URL Blocking	0	0
Venezuela		
Historic: Subscriber Information	1,934	864
IP/URL Blocking	0	0
Mexico		
Historic: Subscriber Information/Call Detail Records	**6,134**	**5,509**
Location Information (Cell Site)	4,138	4,319
Real-Time	**427**	**455**
Pen Registers/Wiretaps/Cell Site	279	232
Location Information (Precise)	148	223
Demands Rejected/Partial or No Data Provided	**1,565**	**1,421**
(Breakout detail of data included in Total Mexico Demands)		
Rejected/Challenged	590	179
Partial or No Information	975	1,242

Additional Resources

You'll find more on our commitment to privacy in:

- Our Privacy Policy
- Our issues brief on Privacy
- Our issues brief on Freedom of Expression