AT&T
Transparency Report

Introduction

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 the laws of the country where your service is provided.

Like all companies, we are required by law to provide information to government and law enforcement agencies, 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

AT&T's first Transparency Report provided information for 2013. In fulfillment of our commitment to issue reports on a semiannual basis, this report provides specific information regarding the number and types of demands to which we responded from Jan. 1, 2014 through June 30, 2014, as well as National Security Demands for the second half of 2013 which we are providing subject to the U.S. Department of Justice's guidelines. This report doesn't include any numbers or information for Cricket™ Wireless because they weren't acquired until March 2014. We plan to include Cricket's data in our next report.

What's New?

We appreciate the comments we received on AT&T's first Transparency Report. We have incorporated changes to provide you with more transparency. These changes include:

- Disclosing the specific number of wiretaps, pen registers, and general court orders processed.
- A clearer statement that we require a search warrant or probable cause order before providing any stored content.

The chart below includes hyperlinks to additional information on the category of data reported.

NATIONAL SECURITY DEMANDS

National Security Letters (Jan. 1 – June 30, 2014)	
▪ Total Received	1,000-1,999
▪ Number of Customer Accounts	2,000-2,999
Foreign Intelligence Surveillance Act (July 1 – Dec. 31, 2013) [1]	
▪ Total Content	0-999
○ Customer Accounts	33,000-33,999
▪ Total Non-Content	0-999
○ Customer Accounts	0-999

TOTAL U.S. CRIMINAL & CIVIL LITIGATION DEMANDS

Total Demands (Federal, State and Local; Criminal and Civil)			**115,925**
▪ Subpoenas		**86,943**	
○ Criminal	78,975		
○ Civil	7,968		
▪ Court Orders (General)		**15,105**	
○ Historic	12,569		
○ Real-time (Pen registers)	2,536	**9,393**	
▪ Search Warrants/Probable Cause Court Orders			
○ Historic			
▪ Stored Content	2,532		
▪ All Others	6,861		
○ Real-Time		**4,484**	
▪ Wiretaps	1,167		
▪ Mobile Locate Demands	3,317		

[1] The Department of Justice imposes a six-month delay for reporting this data.

DEMANDS REJECTED/PARTIAL OR NO DATA PROVIDED

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

Total		**31,097**
▪ Rejected/Challenged	2,110	
▪ Partial or No Information	28,987	

LOCATION DEMANDS

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

Total		**30,886**
▪ Historical	23,646	
▪ Real-time	6,956	
▪ Cell Tower Searches	284	

EMERGENCY REQUESTS

Total		**50,232**
▪ 911	39,449	
▪ Exigent	10,783	

INTERNATIONAL DEMANDS

Total Demands		**17**
▪ Law Enforcement	11	
▪ URL/IP Blocking	6	

Explanatory Notes

NATIONAL SECURITY DEMANDS

The Department of Justice's guidance, issued on Jan. 27, 2014, authorized us to report on the receipt of National Security Letters and court orders issued under the Foreign Intelligence Surveillance Act (FISA), with the exception of data, if any, related to the so-called bulk telephony metadata program. *See* http://www.justice.gov/opa/pr/2014/January/14-ag-081.html.

National Security Letters are subpoenas issued by the Federal Bureau of Investigation in regard to counterterrorism or counterintelligence. These subpoenas are limited to non-content information, such as a list of phone numbers dialed or subscriber information.

Court orders issued pursuant to FISA may direct us to respond to government requests for content and non-content data related to national security investigations, such as international terrorism or espionage.

These types of demands have very strict policies governing our ability to disclose the requests. The recent "Statistical Transparency Report Regarding Use of National Security Authorities" published by the Director of National Intelligence on June 26, 2014, does not alter the Department of Justice's Jan. 27, 2014, guidance.
See http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

Consistent with guidance from January 2014, our report includes the range of customer accounts potentially impacted by these National Security Demands.

TOTAL U.S. CRIMINAL & CIVIL LITIGATION 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 the government — federal, state, and local — against an individual arising from an alleged violation of applicable criminal law.

Civil actions include lawsuits involving private parties (i.e., a personal liability case, divorce proceeding, or any type of dispute 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.

We ensure we receive the right type of legal demand.

We receive several 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 federal and state laws and the type of information being 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 court order or search warrant. If the requesting agent has failed to send the correct type of demand, we reject the demand.

Types of Legal Demands

Subpoenas, court orders and search warrants are used to demand information for use in criminal trials, lawsuits, investigations, and other proceedings. If the applicable rules are followed, we're legally required to provide the information.

In this, our second report, we have changed the reporting for "Total U.S. Criminal & Civil Demands" to more accurately reflect 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. They are used in both criminal and civil cases, typically to obtain written business documents such as calling records.

- **General Court Orders** are signed by a judge. We consider "general" court orders as 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 a civil case, a court order may be issued on a "relevant" or "reasonably calculated to lead to the discovery of admissible evidence" standard. For this report, general court orders were used to obtain historical information like billing records or the past location of a wireless device. In criminal cases, they are also used to obtain 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.

- **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 requested is evidence of a crime. Probable cause is viewed as the highest standard to obtain evidence. Except in emergency circumstances, a search warrant or probable cause court order for all real-time location information (i.e., wiretaps and GPS) and stored

content (i.e., text and voice messages) is required for all jurisdictions, courts, and agencies.

DEMANDS 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 requesting 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 court orders and search warrants we received by the type of location information (historical and real-time) they requested. We also provide the number of requests we received for cell tower searches, which ask us to provide all telephone numbers registered to a particular cell tower for a certain period of time (or to confirm whether a particular telephone number registered on a particular cell tower at a given 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. In our last report, we disclosed the total number of cell tower searches. For clarity, we are now disclosing the total numbers of demands and the total number of searches. For instance, if we received one court order that included ID numbers for two cell towers, we count that as one demand for two searches. For the 284 cell tower demands during this period, we performed 708 searches. We also maintain a record of the average time period that law enforcement requests for one cell tower search, which was 2 hours, 23 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 specific location information. The legal standard required for the production of other location data is unsettled. Some courts have

decided that a general court order is sufficient legal process for law enforcement to obtain such location data. Other courts have determined that the Fourth Amendment requires law enforcement to first obtain a search warrant or probable cause court order before seeking this location information. With the exception of emergency situations, we require an order signed by a judge before producing any type of location information to law enforcement. We will continue to follow these legal developments and, in all circumstances, we will comply with the applicable law.

EMERGENCY REQUESTS

This category includes the number of times we responded to 911-related inquiries and "exigent requests" to help locate or identify a 911 caller. These are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies. The numbers provided in this category are the total of 911 and exigent searches that we processed during this reporting period.

Even when responding to an emergency, we protect your privacy:

- When responding to 911 inquiries, we confirm the request is coming from a legitimate Public Safety Answering Point before quickly responding.
- For exigent requests, we receive a certification from a law enforcement agency confirming they are dealing with a case involving risk of death or serious injury before we share information.

INTERNATIONAL DEMANDS

International Demands represent the number of demands we received from governments outside the U.S., and relate to AT&T's global business operations in these countries. Such International Demands are for customer information stored in their countries, and URL/IP (website/Internet address) blocking requests.

We are not a content provider outside the U.S. but are required by some countries' laws to comply with requests to block access to websites that are deemed offensive, illegal, unauthorized or otherwise inappropriate in certain countries. These requests might be designed to block sites related to displaying child pornography, unregistered and illegal gambling, defamation, illegal sale of medicinal products, or trademark and copyright infringement. A demand may request that one or more identifiers (i.e., IP addresses or URLs) be blocked.

The majority of law enforcement demands involve requests for information relating to individuals. Because our global operations support only very large multi-national business customers, we received relatively few international demands. We do not have a mobility network outside the U.S., and we don't provide services to individual consumers residing outside the U.S. We received no demands from the U.S. government for data stored outside the U.S. If we receive an international demand for information stored in the U.S., we refer it to that country's Mutual Legal Assistance Treaty (MLAT) process. The Federal Bureau of Investigation 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 Federal Bureau of Investigation demand we may receive.

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.