

Comcast Transparency Report
July 2014 – December 2014

Comcast has released its third Transparency Report disclosing information on the volume and categories of requests for customer information made by U.S. law enforcement and national security agencies at the federal, state, and local government levels in the second half of 2014. Requests for information made under the Foreign Intelligence Surveillance Act (FISA) are subject to a six-month delay, so the information listed in that category covers the first half of 2014.

While Comcast is legally obligated to respond to lawful requests for customer-related information by these government agencies, we are committed to protecting our customers' privacy. Accordingly, we carefully scrutinize each government request seeking access to customer data. Before providing any information to the government, we make sure that the request is appropriately tailored and that our response accords with governing law.

This Report provides the number of national security data requests that we receive in bands of 1,000, consistent with the guidance provided by the Department of Justice on the format and scope of such reports. We make this data available to the public in order to help enhance the transparency of government surveillance programs and to promote an open dialogue about the important privacy, law enforcement, and national security issues raised by those programs. In the meantime, we will continue to safeguard our customers' privacy rights and ensure that our responses to government requests for information meet all applicable legal requirements.

Criminal Demands July 1, 2014 – December 31, 2014	
Subpoenas	8,208
Court Orders:	
General Orders	1,598
Pen Register/Trap & Trace	77
Wiretaps	6
Warrants:	
Content Warrants	103
Non-Content Warrants	602
Total	10,594

Emergency Requests July 1, 2014 – December 31, 2014	530
--	-----

National Security Demands	
National Security Letters (July 1, 2014 – December 31, 2014)	0-999
Number of Customer Accounts Impacted	0-999
Foreign Intelligence Surveillance Act (January 1, 2014 – June 30, 2014) Content and Non-Content	0-999
Number of Customer Accounts Impacted	0-999

Definitions (as terms appear in the Report)

Subpoenas typically seek basic customer account information that is contained in the business records of a service provider. Frequently, subpoenas seek the identification of a customer account by name and address based on a telephone number or Internet Protocol address assigned to the account. An officer of the court, such as a law enforcement officer or a prosecuting attorney, for example, usually signs a subpoena.

Court Orders typically seek historical information and more detailed information than is available using a subpoena. A judge signs a court order indicating that the law enforcement entity seeking it has made the requisite showing under the law to obtain the order.

General Orders are court orders except for wiretap, pen register, and trap and trace orders. Most general orders seek information similar to that available with a subpoena, and some also seek contents of communications.

Pen Register Orders seek real time access to information like phone numbers and e-mail addresses as they are dialed or sent, and Trap and Trace Orders seek real time access to incoming phone numbers or e-mail addresses.

Wiretap Orders seek real time access to the contents of communications.

Warrants typically seek information similar to that available under subpoenas and some court orders, but may also seek the contents of communications in certain cases. A judge signs a warrant based on a showing by the law enforcement entity seeking it that there is probable cause that the information sought by the warrant is evidence of a crime.

Emergency Requests typically seek information from a service provider on an expedited basis in an emergency involving danger of death or serious physical injury to any person. Our policy requires the requesting law enforcement officer to provide a written certification describing the emergency. Comcast uses this information to verify an emergency request in connection with responding to it. Some emergency requests seek information related to 911 telephone calls. In those cases, Comcast verifies that the request is coming from a legitimate Public Service Answering Point before responding to it.

National Security Letters are issued by the Federal Bureau of Investigation. The FBI issues these in connection with counter-terrorism or counter-intelligence matters; national security letters are limited to seeking non-content information like customer account information.

Foreign Intelligence Surveillance Act Orders and Warrants are issued by the Foreign Intelligence Surveillance Court. These orders and warrants typically seek both content and non-content information relating to national security matters, such as international terrorism or espionage.

Customer Accounts Affected means the number of unique Comcast subscriber accounts affected by a particular legal request. For example, one national security letter may seek information about two different subscriber accounts.

Content refers to the actual contents of a communication, such as the body of an e-mail or a telephone conversation.

Non-Content refers to information other than the contents of a communication, such as a list of phone numbers or e-mail addresses or header information (signaling, addressing, or routing information).