Update on National Security and Law Enforcement Orders

January 27, 2014

Apple has been working closely with the White House, the U.S. Attorney General, congressional leaders, and the Department of Justice to advocate for greater transparency with regard to the national security orders we receive. We believe strongly that our customers have the right to understand how their personal information is being handled, and we are pleased the government has developed new rules that allow us to more accurately report law enforcement orders and national security orders in the U.S.

We work hard to deliver the most secure hardware and software in the world and we will continue to provide our customers with the best privacy protections available. Personal conversations are protected using end-to-end encryption over iMessage and FaceTime, and Apple does not store location data, Maps searches, or Siri requests in any identifiable form.

Apple is reporting the actual number of requests for information related to law enforcement investigations. Law enforcement requests most often relate to criminal investigations such as robbery, theft, murder, and kidnapping. In addition, Apple is re-reporting all the national security orders we have received, including orders received under FISA and National Security Letters (NSLs), to reflect the new guidelines that allow us to report these orders separate from law enforcement orders, in bands of 250. This data represents every U.S. national security order for data about our customers regardless of geography. We did not receive any orders for bulk data. The number of accounts involved in national security orders is infinitesimal relative to the hundreds of millions of accounts registered with Apple.

Apple reviews each order, whether criminal or under a national security authority, to ensure that it is legally issued and as narrowly tailored as possible. If there is any question about the legitimacy or scope of the order, we challenge it. Only when we are satisfied that the order is valid and appropriate do we deliver the narrowest possible set of information in response to that order.

National Security Letters (NSLs), which are often the first step in an investigation, do not require a court order but by law they may not be used to obtain customer content. NSLs are limited to transactional data such as a customer's contact information. Apple is required by law to comply with these NSLs if we have the information requested.

The information provided below replaces the U.S. data in Apple's November 5, 2013 Report on Government Information Requests, which details the Account Information Requests and Device Information Requests we have received worldwide from January 1, 2013 to June 30, 2013.

National Security Orders

Total National Security Orders Received	Total Accounts Affected
0 - 249	0 - 249

Account Information Requests

Country	Total Number of Law Enforcement Account Requests Received	Number of Accounts Specified in the Requests	Number of Accounts for Which Data Was Disclosed	Number of Account Requests Where Apple Objected	Number of Account Requests Where No Data Was Disclosed	Number of Account Requests Where Non-Content Data Was Disclosed	Number of Account Requests Where Some Content Was Disclosed	Percentage of Account Requests Where Some Data Was Disclosed[1]
United States of America	927	2,330	747	102	254	601	71	72%

[1] This chart was updated on May 25, 2018 to correct the Percentage of Account Requests Where Some Data Was Disclosed, which had a calculation error. All other data was presented correctly.