Report on Government Information Requests

November 5, 2013

We believe that our customers have a right to understand how their personal information is handled, and we consider it our responsibility to provide them with the best privacy protections available. Apple has prepared this report on the requests we receive from governments seeking information about individual users or devices in the interest of transparency for our customers around the world.

This report provides statistics on requests related to customer accounts as well as those related to specific devices. We have reported all the information we are legally allowed to share, and Apple will continue to advocate for greater transparency about the requests we receive.

Protecting Personal Data

Apple offers customers a single, straightforward privacy policy that covers every Apple product. Customer privacy is a consideration from the earliest stages of design for all our products and services. We work hard to deliver the most secure hardware and software in the world, including such innovative security solutions as Find My iPhone and Touch ID, which have made the iPhone both more secure and more convenient.

Perhaps most important, our business does not depend on collecting personal data. We have no interest in amassing personal information about our customers. We protect personal conversations by providing end-to-end encryption over iMessage and FaceTime. We do not store location data, Maps searches, or Siri requests in any identifiable form.

Advocating for Greater Transparency

At the time of this report, the U.S. government does not allow Apple to disclose, except in broad ranges, the number of national security orders, the number of accounts affected by the orders, or whether content, such as emails, was disclosed. We strongly oppose this gag order, and Apple has made the case for relief from these restrictions in meetings and discussions with the White House, the U.S. Attorney General, congressional leaders, and the courts. Despite our extensive efforts in this area, we do not yet have an agreement that we feel adequately addresses our customers' right to know how often and under what circumstances we provide data to law enforcement agencies.

We believe that dialogue and advocacy are the most productive way to bring about a change in these policies, rather than filing a lawsuit against the U.S. government. Concurrent with the release of this report, we have filed an Amicus brief at the Foreign Intelligence Surveillance Court (FISA Court) in support of a group of cases requesting greater transparency. Later this year, we will file a second Amicus brief at the Ninth Circuit in support of a case seeking greater transparency with respect to National Security Letters. We feel strongly that the government should lift the gag order and permit companies to disclose complete and accurate numbers regarding FISA requests and National Security Letters. We will continue to aggressively pursue our ability to be more transparent.

Requests from Law Enforcement

Like many companies, Apple receives requests from law enforcement agencies to provide customer information. As we have explained, any government agency demanding customer content from Apple must get a court order.[1] When we receive such a demand, our legal team carefully reviews the order. If there is any question about the legitimacy or scope of the court order, we challenge it. Only when we are satisfied that the court order is valid and appropriate do we deliver the narrowest possible set of information responsive to the request.

Unlike many other companies dealing with requests for customer data from government agencies, Apple's main business is not about collecting information. As a result, the vast majority of the requests we receive from law enforcement seek information about lost or stolen devices, and are logged as **device requests**. These types of requests frequently arise when our customers ask the police to assist them with a lost or stolen iPhone, or when law enforcement has recovered a shipment of stolen devices.

Only a small fraction of the requests that Apple receives seek personal information related to an iTunes, iCloud, or Game Center account. Account-based requests generally involve account holders' personal data and their use of an online service in which they have an expectation of privacy, such as government requests for customer identifying information, email, stored photographs, or other user content stored online. Apple logs these as **account requests**.

We believe it is important to differentiate these categories and report them individually. Device requests and account requests involve very different types of data. Many of the device requests we receive are initiated by our own customers working together with law enforcement. Device requests never include national security–related requests.

Reporting the Number of Requests for Information About Customer Accounts

The following tables detail the account requests and device requests Apple received from law enforcement agencies between January 1, 2013, and June 30, 2013.

Table 1 shows account requests. The U.S. government has given us permission to share only a limited amount of information about these orders, with the requirement that we combine national security orders with account-based law enforcement requests and report only a consolidated range in increments of 1000.

The most common account requests involve robberies and other crimes or requests from law enforcement officers searching for missing persons or children, finding a kidnapping victim, or hoping to prevent a suicide. Responding to an account request usually involves providing information about an account holder's iTunes or iCloud account, such as a name and an address. In very rare cases, we are asked to provide stored photos or email. We consider these requests very carefully and only provide account content in extremely limited circumstances.

Table 2 shows device requests. Even though device requests have not been the focus of public debate, we are disclosing them to make our report as comprehensive as possible. These may include requests for the customer contact information provided to register a device with Apple or the date the device first used Apple services. We count devices based on the individual serial numbers related to an investigation.

For further information about data in these tables, please see the glossary below.

[1] National Security Letters (NSLs), which are often the first step in an investigation, do not carry a court order but by law they may not be used to obtain customer content. NSL orders are limited to transactional data such as a customer's contact information. Apple is required by law to comply with these requests if we have the information being sought. Apple assesses the legitimacy of each NSL as if it were a regular court order.

Table 1: Account Information Requests

Country [2]	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 Non-Content Data Was Disclosed	Number of Account Requests Where No Data Was Disclosed	Number of Account Requests Where Some Content Was Disclosed	Percentage of Account Requests Where Some Data Was Disclosed
Australia	74	75	41	22	34	40	0	54%
Austria	2	2	1	1	1	1	0	50%
Bahamas	1	1	1	0	0	1	0	100%
Belarus	1	1	0	1	1	0	0	0%
Belgium	13	20	4	8	8	5	0	38%
Brazil	8	8	0	8	8	0	0	0%
Canada	6	6	4	0	2	4	0	67%
China	6	6	2	4	4	2	0	33%
Czech Republic	2	2	1	1	1	1	0	50%
Denmark	11	11	6	5	5	6	0	55%
France	71	72	14	49	54	17	0	24%
Germany	93	93	5	86	87	6	0	6%
Hong Kong	32	33	25	4	8	24	0	75%
Ireland	5	5	3	2	2	3	0	60%
Italy	60	76	18	34	38	22	0	37%
Japan	42	49	3	21	32	10	0	24%
Netherlands	4	4	1	3	3	1	0	25%
New Zealand	3	3	1	2	2	1	0	33%
Norway	6	6	2	4	4	2	0	33%
Poland	1	2	0	1	1	0	0	0%
Portugal	2	2	2	0	0	2	0	100%
Russia	1	1	1	0	0	1	0	100%
San Marino	2	2	0	2	2	0	0	0%
Singapore	23	23	13	9	10	13	0	57%
South Korea	4	4	2	2	2	2	0	50%
Spain	102	104	19	77	80	22	0	22%
Sweden	7	7	3	3	4	3	0	43%
Switzerland	6	6	1	4	5	1	0	17%
Taiwan	4	4	1	1	1	3	0	75%
United Kingdom	127	141	51	79	80	46	1	37%
United States	1000-2000	2000-3000	0-1000	0-1000	0-1000	0-1000	0-1000	—

[2] Personal information regarding individuals who reside in a member state of the European Economic Area (EEA) is controlled by Apple Distribution International in Cork, Ireland, and processed on its behalf by Apple Inc. Personal information collected in the EEA when using iTunes is controlled by iTunes SARL in Luxembourg and processed on its behalf by Apple Inc. All personally identifiable content is hosted on servers within the United States. Accordingly, law enforcement agencies outside the United States seeking such content must obtain legal process through U.S. authorities. Where the foreign country has signed a Mutual Legal Assistance Treaty (MLAT) with the United States, then appropriate legal process can be obtained through the process specified in the treaty or through other cooperative efforts with the U.S. Department of Justice.

Table 2: Device Information Requests

Country[2]	Total Number of Law Enforcement Device Requests Received	Number of Devices Specified in the Requests	Number of Device Requests Where Some Data Was Provided	Percentage of Device Requests Where Some Data Was Provided
Australia	1178	1929	695	59%
Austria	49	104	39	80%
Bahamas	1	1	1	100%
Belgium	64	175	41	64%
Brazil[3]	34	5057	2	6%
Canada	38	224	35	92%
Chile	1	1	1	0%
China	585	1268	429	73%
Cyprus	1	1	0	0%
Czech Republic	12	99	7	58%
Denmark	55	132	41	75%
Estonia	1	1	0	0%
Finland	3	4	2	67%
France	530	2679	334	63%
Germany	2156	4928	1856	86%
Greece	2	8	2	100%
Hong Kong	92	267	64	70%
Hungary	12	13	3	25%
India	27	65	11	41%
Ireland	102	379	79	77%
Italy	409	4034	331	81%
Japan	106	182	12	11%
Luxembourg	67	92	29	43%
Malaysia	1	2	0	0%
Netherlands	61	229	40	66%
New Zealand	71	116	42	59%
Norway	33	101	27	82%
Poland	2	53	1	50%
Portugal	17	300	14	82%
Russia	13	15	12	92%
Singapore	1498	1681	853	57%
Slovenia	4	5	2	50%
South Korea	88	419	46	52%
Spain	308	463	244	79%
Swaziland	1	1	0	0%
Sweden	61	102	54	89%
Switzerland	107	139	91	85%
Taiwan	81	115	10	12%
United Arab Emirates	1	1	1	100%
United Kingdom	1028	2474	689	67%
United States	3542	8605	3110	88%

[2] Personal information regarding individuals who reside in a member state of the European Economic Area (EEA) is controlled by Apple Distribution International in Cork, Ireland, and processed on its behalf by Apple Inc. Personal information collected in the EEA when using iTunes is controlled by iTunes SARL in Luxembourg and processed on its behalf by Apple Inc. All personally identifiable content is hosted on servers within the United States. Accordingly, law enforcement agencies outside the United States seeking such content must obtain legal process through U.S. authorities. Where the foreign country has signed a Mutual Legal Assistance Treaty (MLAT) with the United States, then appropriate legal process can be obtained through the process specified in the treaty or through other cooperative efforts with the U.S. Department of Justice.

[3] Five requests are related to the recovery of stolen cargoes of devices.

Notes

Apple keeps track of every request we receive. Some countries are not listed in this report because Apple has not received any information requests from the government there.

The number of affected accounts and devices is often larger than the number of requests because law enforcement may seek information related to multiple accounts or devices. For example, some device requests related to the theft of a shipment may involve hundreds of serial numbers.

In cases where no data was disclosed, Apple may have objected to a government request for legal reasons or searched our records and discovered that we have no relevant information. This category includes multiple scenarios in which no data was disclosed.

Apple has never received an order under Section 215 of the USA Patriot Act. We would expect to challenge such an order if served on us.

Glossary of Terms

Table 1 Definitions

Total Number of Law Enforcement Account Requests Received

The total number of account-based requests issued by a government agency and/or a court that are received by Apple and seek customer data related to specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers. Account-based law enforcement requests come in various forms such as subpoenas, court orders, and warrants.

Number of Accounts Specified in the Requests

The number of discernible accounts, based on specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers in each law enforcement request. A single request may involve multiple accounts where, for example, multiple accounts are associated with the same credit card.

Number of Accounts for Which Data Was Disclosed

The number of discernible accounts, based on specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers, for which Apple provided some iCloud, iTunes, or Game Center data.

Number of Account Requests Where Apple Objected

The number of law enforcement requests that resulted in Apple refusing to provide some data based on various grounds, such as jurisdiction, improper process, insufficient process, invalid process, or where the scope of the request was excessively broad. For example, Apple may object to a law enforcement request as “invalid” if it was not signed.

Number of Account Requests Where Non-Content Data Was Disclosed

The number of law enforcement requests that resulted in Apple providing only subscriber or transactional information, but not content. For example, Apple may provide subscriber information and a limited purchase history in response to valid legal process.

Number of Account Requests Where No Data Was Disclosed

The number of law enforcement requests that resulted in Apple providing no customer information whatsoever.

Number of Account Requests Where Some Content Was Disclosed

The number of law enforcement requests where Apple determined that an account request was lawful and provided content such as iCloud email, contacts, calendar, or Photo Stream content. Apple only provides user account content in extremely limited circumstances.

Percentage of Account Requests Where Some Data Was Disclosed

The percentage of law enforcement requests that resulted in Apple providing some iCloud, iTunes, or Game Center data.

Table 2 Definitions

Total Number of Law Enforcement Device Requests Received

The number of device-based requests issued by a government agency and/or a court that are received by Apple and seek customer data related to specific device identifiers such as serial or IMEI numbers. Law enforcement device requests come in various forms such as subpoenas, court orders, and warrants. A single request may involve multiple devices. For example, in the case of a recovered shipment of stolen devices, law enforcement may seek information related to several devices in a single request.

Number of Devices Specified in the Requests

The total number of iPhone, iPad, iPod, Mac, or other devices identified in each law enforcement request, based on the number of device identifiers. For example, law enforcement agencies investigating theft cases often send requests seeking information based on serial numbers. Each serial number is counted as a single device. A request may involve multiple devices as in the case of a recovered shipment of stolen devices.

Number of Device Requests Where Some Data Was Provided

The number of law enforcement requests that resulted in Apple providing relevant device information, such as registration, subscriber, service, repair, and purchase information in response to valid legal process.

Percentage of Device Requests Where Some Data Was Provided

The percentage of law enforcement requests that resulted in Apple providing some relevant device information in response to valid legal process.