



Report on Government Information Requests

July 1 - December 31, 2015

Apple takes our commitment to protecting your data very seriously and we work incredibly hard to deliver the most secure hardware, software and services available. We also believe every customer has a right to understand how their personal information is handled.

For government information requests, we report as much detail as we are legally allowed. When we receive an account request from law enforcement requesting a customer's personal information, we will notify the customer a request concerning their personal data was made unless we are explicitly prohibited from doing so. We are reserving the right to make exceptions, such as for extreme situations when we believe disclosing information could put a child or other person in serious danger, or where notice is not applicable to the underlying facts of the case.

Any government agency demanding customer content from Apple must get a search warrant. When we receive such a demand, our legal team carefully reviews it. If there's a question about the legitimacy or scope of the request we challenge it, as we have done as recently as this year. We only comply with information requests once we are satisfied that the request is valid and appropriate, and then we deliver the narrowest possible set of information.

How We Report Requests

The following tables detail device requests, account requests, emergency requests, National Security Orders, and requests for account deletion Apple received from July 1 through December 31, 2015.

Device Requests

Table 1 shows device requests. The vast majority of the requests we receive from law enforcement relate to information about lost or stolen devices, and we report these as device requests. Device requests may include requests for customer contact information provided to register a device with Apple or the date(s) the device used Apple services. We count devices based on the individual serial or IMEI numbers related to an investigation. We encourage any customer who suspects their device is stolen to contact their local law enforcement agency.

Account Requests

Table 2 shows account requests. 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 certain cases, we are asked to provide customers' iCloud content, which may include stored photos, email, iOS device backups, documents, contacts, calendars, and bookmarks. We consider these requests very carefully and provide account content when the legal request is a search warrant.

Emergency Requests

Table 3 shows all the emergency and/or exigent requests that we have received globally. Pursuant to 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4) Apple may voluntarily disclose information, including contents of communications and customer records, to a federal, state, or local governmental entity if Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay. The number of emergency requests that Apple deemed to be exigent and responded to is detailed in Table 3.

National Security Orders

Table 4 shows all the national security orders we have received, including orders received under FISA and National Security Letters ("NSLs"). To date, Apple has not received any orders for bulk data. We report all the national security orders we have received, including orders received under FISA and NSLs, in bands of 250. Though we want to be more specific, this is currently the narrowest range allowed by the government.

Account Deletion Requests

Table 5 shows the number of account deletion requests we have received and how often we have complied with these requests.



Table 1: Device Requests July 1 - December 31, 2015

Country	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
Asia Pacific				
Australia	3004	4617	2072	69%
China	1005	2413	668	66%
Hong Kong	651	995	450	69%
Indonesia	3	4	1	33%
Japan	225	324	109	48%
Malaysia	5	39	5	100%
New Zealand	311	355	233	75%
Singapore	1936	2065	962	50%
South Korea*	119	27922	71	60%
Taiwan	37	39	14	38%
Thailand	4	4	1	25%
Asia Pacific Total	7300	38777	4586	63%
Europe, Middle East, India, Africa				
Austria	70	100	44	63%
Belgium	107	221	56	52%
Bulgaria	1	2	0	0%
Czech Republic	32	6331	22	69%
Denmark	102	246	73	72%
Finland	6	7	5	83%
France	1610	3679	562	35%
Germany	11989	31360	6281	52%
Greece	11	17	8	73%
Hungary	31	1051	18	58%
Iceland	7	8	5	71%
India	37	52	7	19%
Ireland	252	671	190	75%
Italy	966	2109	600	62%
Liechtenstein	1	1	1	100%
Luxembourg	32	40	12	38%
Malta	2	2	1	50%
Monaco	1	1	0	0%
Netherlands	39	341	16	41%
Norway	63	122	37	59%
Poland**	22	56447	12	55%
Portugal	233	274	49	21%
Romania	2	13	0	0%
Russia	58	95	20	34%
Saudi Arabia	1	1	0	0%
Slovakia	3	12	3	100%
Slovenia	69	90	31	45%
South Africa	3	4	0	0%
Spain	1196	3460	744	62%
Sweden	205	443	137	67%
Switzerland	136	501	85	63%
Turkey	63	272	33	52%
Uganda	1	1	0	0%
Ukraine	2	3	0	0%
United Kingdom	1969	3830	1075	55%
Europe, Middle East, India, Africa Total	19322	111807	10127	52%
Latin America				
Brazil	55	357	44	80%
Uruguay	1	1	1	100%
Latin America Total	56	358	45	80%
North America				
Canada	9	36	6	67%
United States of America	4000	16112	3195	80%
North America Total	4009	16148	3201	80%

*South Korea: predominantly stolen devices

**Poland: predominately requests from Customs and Revenue Authorities



Table 2: Account Requests July 1 - December 31, 2015

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
Asia Pacific								
Australia	91	116	37	51	61	30	0	33%
China*	32	6724	5082	9	15	17	0	53%
Hong Kong	13	15	7	0	6	7	0	54%
Japan	55	67	34	30	28	27	0	49%
New Zealand	6	9	0	5	6	0	0	0%
Singapore	15	24	20	4	4	11	0	73%
South Korea	6	8	2	4	4	2	0	33%
Taiwan	5	10	7	0	2	3	0	60%
Asia Pacific Total	223	6973	5189	103	126	97	0	43%
Europe, Middle East, India, Africa								
Austria	12	12	8	3	4	8	0	67%
Belgium	6	8	4	2	3	3	0	50%
Cyprus	1	1	0	0	1	0	0	0%
Czech Republic	5	5	1	3	4	1	0	20%
Denmark	4	4	1	3	3	1	0	25%
Finland	3	3	2	1	1	2	0	67%
France	60	65	18	25	42	18	0	30%
Germany	130	150	72	41	62	68	0	52%
India	3	5	4	0	1	2	0	67%
Ireland	8	8	5	2	3	5	0	63%
Italy	26	31	8	12	19	7	0	27%
Kuwait	1	1	0	1	1	0	0	0%
Luxembourg	2	2	1	0	1	1	0	50%
Malta	1	1	0	1	1	0	0	0%
Netherlands	13	13	5	1	8	5	0	38%
Norway	5	6	4	1	2	3	0	60%
Portugal	7	8	5	2	3	4	0	57%
Russia	3	3	0	3	3	0	0	0%
Spain	21	21	10	5	11	10	0	48%
Sweden	6	6	2	3	4	2	0	33%
Switzerland	8	8	3	4	5	3	0	38%
Turkey	3	3	2	0	1	2	0	67%
United Kingdom	208	248	135	45	87	121	0	58%
Europe, Middle East, India, Africa Total	536	612	290	158	270	266	0	50%
Latin America								
Brazil	32	63	56	4	1	13	18	97%
Dominican Republic	1	1	1	0	0	1	0	100%
Latin America Total	33	64	57	4	1	14	18	97%
North America								
Canada	6	9	9	2	0	6	0	100%
United States of America	1015	5192	4411	116	184	509	322	82%
North America Total	1021	5201	4420	118	184	515	322	82%

*China: predominantly accounts related to phishing investigations

**Table 3: Emergency Requests July 1 - December 31, 2015**

Country	Total Number of Emergency Requests Received
Asia Pacific	
Australia	2
Japan	2
Europe, Middle East, India, Africa	
Denmark	1
Finland	1
France	4
Germany	3
Ireland	1
Italy	2
Nepal	1
Netherlands	3
Switzerland	2
United Kingdom	43
Latin America	
Chile	1
North America	
Canada	6
United States of America	106
Total	178

Table 4: National Security Requests July 1 - December 31, 2015

	7/1/2015 - 12/31/2015
National Security Orders Received	1250-1499
Total Accounts Affected	1000-1249

Table 5: Account Deletion Requests by Government July 1 - December 31, 2015
(Court order or search warrant required)

Number of Account Deletion Requests Received	Number of Account Deletion Requests Where Apple Objected	Number of Account Deletion Requests Where Account Was Deleted
3	0	3



Glossary of Terms

Table 1 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.

Table 2 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, for example, where 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 data, for example, 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 were not signed.

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 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 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 data, for example, iCloud, iTunes, or Game Center data.