

Report on Government and Private Party Requests for Customer Information

January 1 - June 30, 2018

Introduction

Apple is very seriously committed to protecting your data and we work hard to deliver the most secure hardware, software and services available. We believe our customers have a right to understand how their personal data is managed and protected. This report provides information regarding requests Apple received from government agencies worldwide and U.S. private parties from January 1 through June 30, 2018.

Types of requests we receive

Apple receives various forms of legal requests seeking information from or actions by Apple. We receive requests from governments globally where we operate and from private parties.

Government request circumstances can vary from instances where law enforcement agencies are working on behalf of customers who have requested assistance regarding lost or stolen devices, to instances where law enforcement are working on behalf of customers who suspect their credit card has been used fraudulently to purchase Apple products or services, to instances where an account is suspected to have been used unlawfully. Requests can also seek to preserve an Apple account, restrict access to an Apple account or delete an Apple account. Additionally, requests can relate to emergency situations where there is imminent harm to the safety of any person.

Private party request circumstances generally relate to instances where private litigants are involved in either civil or criminal proceedings.

Types of legal requests Apple receives from the United States can be: subpoenas, court orders, search warrants, pen register/trap and trace orders, or wiretap orders.

Types of legal requests Apple receives internationally can be: Production Orders (Australia, Canada), Tribunal Orders (New Zealand), Requisition or Judicial Rogatory Letters (France), Solicitud Datos (Spain), Ordem Judicial (Brazil), Auskunftersuchen (Germany), Obligation de dépôt (Switzerland), 個人情報の開示依頼 (Japan), Personal Data Request (United Kingdom), as well as equivalent court orders and/or requests from other countries.

Types of customer data sought in requests

The type of customer data sought in requests varies depending on the case under investigation. For example, in stolen device cases, law enforcement generally seek details of customers associated with devices or device connections to Apple services. In credit card fraud cases, law enforcement generally seek details of suspected fraudulent transactions. Depending on what the legal request asks, Apple will provide subscriber or transaction details in response to valid legal requests received.

In instances where an Apple account is suspected of being used unlawfully, law enforcement may seek details of the customer associated with the account, account connections or transaction details or account content. Any U.S. government agency seeking customer content data from Apple must obtain a search warrant issued upon a showing of probable cause. International requests for content must comply with applicable laws, including the U.S. Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or Agreement with the U.S. is in compliance with ECPA.

The type of customer data sought in emergency situations generally relates to details of customers' connection to Apple services. We have a dedicated team available around the clock to respond to emergency requests. Apple processes emergency requests from law enforcement globally on a 24/7 basis. An emergency request must relate to circumstances involving imminent danger of death or serious physical injury to any person. If Apple believes in good faith that it is a valid emergency, we may voluntarily provide information to law enforcement on an emergency basis.



How we manage and respond to requests

Apple has a centralized and standardized process for receiving, tracking, processing, and responding to legal requests from law enforcement, government, and private parties worldwide, from when a request is received until when a response is provided.

Government and private entities are required to follow applicable laws and statutes when requesting customer information and data. We contractually require our service providers to abide by the same standard for any government information requests for Apple data. Our legal team reviews requests received to ensure that the requests have a valid legal basis. If they do, we comply with the requests and provide data responsive to the request. If we determine a request does not have a valid legal basis, or if we consider it to be unclear, inappropriate and/or over-broad, we challenge or reject it.

How we count requests and responses

Apple counts requests received from government agencies worldwide and United States private parties within the reporting period in which they are received. Overall numbers of requests and responses are reported.

A request with a valid legal basis is processed and responded to, and is counted as one request. A request that is challenged/rejected is counted as one request. Where new legal process is submitted to amend the request, it is counted as a new request. We count each request we challenge or reject for account-based, account restriction/deletion, emergency and private party requests; and report these numbers accordingly.

We count the number of discernible devices, financial identifiers, and/or accounts specified in requests, and report these accordingly by type. If there are two identifiers for one device in a request, for example a serial number and IMEI number, we count this as one device. If there are multiple identifiers for one account in a request, for example Apple ID, full name and phone number, we count this as one account.

For United States Government Requests by Legal Process Type reporting, where two types of legal process are combined in a single request, such as a search warrant with an incorporated court order, we record the request at the highest level of legal process and the request would be reported as a search warrant. An exception is where a pen register/trap and trace order is received; this is counted as a pen register/trap and trace order, notwithstanding that it may include a search warrant.

How we report requests and responses

We report on requests and responses in the following categories:

- 1) Worldwide Government Device Requests
- 2) Worldwide Government Financial Identifier Requests
- 3) Worldwide Government Account Requests
- 4) Worldwide Government Account Preservation Requests
- 5) Worldwide Government Account Restriction/Deletion Requests
- 6) Worldwide Government Emergency Requests
- 7) United States Government National Security Requests
- 8) United States Government Device Requests by Legal Process Type
- 9) United States Government Financial Identifier Requests by Legal Process Type
- 10) United States Government Account Requests by Legal Process Type
- 11) United States Private Party Requests for Information
- 12) United States Private Party Requests for Account Restriction/Deletion

For government agency requests for customer information and data, we report the numbers of requests we receive and our responses in various categories. For United States National Security requests for customer information and data, we report as much detail as we are legally allowed. In order to report FISA non-content and content requests in separate categories, Apple is required by law to delay reporting by 6 months and report the numbers in ranges of 500, pursuant to the USA FREEDOM Act of 2015.

Customer notification

When we receive an account request seeking our customers' information and data, we notify the customer that we have received a request concerning their personal data except where we are explicitly prohibited by the legal process, by a court order Apple receives, or by applicable law. We reserve the right to make exceptions, such as instances where we believe providing notice creates a risk of injury or death to an identifiable individual, or where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case.



**Table 1: Worldwide Government Device Requests
January 1 - June 30, 2018**

Table 1 provides information regarding device-based requests received. Examples of such requests are where law enforcement agencies are working on behalf of customers who have requested assistance regarding lost or stolen devices. Additionally, Apple regularly receives multi-device requests related to fraud investigations. Device-based requests generally seek details of customers associated with devices or device connections to Apple services.

Country or Region	# of Device Requests Received	# of Devices Specified in the Requests	# of Device Requests Where Data Provided	% of Device Requests Where Data Provided
Asia Pacific				
Australia	2,357	3,919	1,987	84%
China	751	30,764	705	94%
Hong Kong	567	900	436	77%
Japan	446	914	378	85%
New Zealand	315	855	271	86%
Singapore	1,689	8,651	1,526	90%
South Korea	92	39,423	74	80%
Taiwan	71	174	46	65%
Thailand	4	5	2	50%
Asia Pacific Total	6,292	85,605	5,425	86%
Europe, Middle East, India, Africa				
Andorra	13	13	12	92%
Austria	502	949	396	79%
Belgium	216	538	171	79%
Czech Republic	30	145	17	57%
Denmark	84	133	69	82%
Estonia	2	2	1	50%
Finland	8	891	5	63%
France	1,179	4,703	913	77%
Germany	13,704	26,160	10,596	77%
Greece	34	151	29	85%
Hungary	18	309	14	78%
India	27	379	17	63%
Ireland	160	227	142	89%
Italy	595	923	448	75%
Kazakhstan	1	2	1	100%
Liechtenstein	6	6	4	67%
Luxembourg	9	73	8	89%
Netherlands	32	97	20	63%
Norway	37	201	24	65%
Poland	32	14,060	26	81%
Portugal	175	211	131	75%
Romania	13	175	9	69%
Russia	702	2,909	536	76%
Serbia	1	1	0	0%
Slovakia	1	1	1	100%
Slovenia	18	168	15	83%
South Africa	23	368	15	65%
Spain	2,276	3,353	1,868	82%
Sweden	136	354	115	85%
Switzerland	344	611	244	71%
Turkey	60	87	32	53%
Ukraine	2	2	1	50%
United Kingdom	572	2,606	440	77%
Europe, Middle East, India, Africa Total	21,012	60,808	16,320	78%
Latin America				
Argentina	7	42	3	43%
Brazil	407	2,324	345	85%
Chile	36	106	27	75%
Paraguay	1	1	1	100%
Latin America Total	451	2,473	376	83%
North America				
Canada	15	23	11	73%
Mexico	2	3	0	0%
United States of America	4,570	14,911	3,697	81%
North America Total	4,587	14,937	3,708	81%
Worldwide Total	32,342	163,823	25,829	80%



of Device Requests Received

The number of device-based requests received from a government agency seeking customer data related to specific device identifiers, such as serial number or IMEI number. Requests can be in various formats such as subpoenas, court orders, warrants, or other valid legal requests. We count each individual request received from each country/region and report the total number of requests received by country/region.

of Devices Specified in the Requests

The number of devices specified in the requests. One request may contain one or multiple device identifiers. For example, in a case related to the theft of a shipment of devices, law enforcement may seek information related to several device identifiers in a single request. We count the number of devices identified in each request, received from each country/region, and report the total number of devices specified in requests received by country/region.

of Device Requests Where Data Provided

The number of device-based requests that resulted in Apple providing data, such as customers associated with devices, device connections to Apple services, purchase, customer service, or repair information, in response to a valid legal request. We count each device-based request where we provide data and report the total number of such instances by country/region.

% of Device Requests Where Data Provided

The percentage of device-based requests that resulted in Apple providing data. We calculate this based on the number of device-based requests that resulted in Apple providing data per country/region, compared to the total number of device-based requests Apple received from that country/region.



**Table 2: Worldwide Government Financial Identifier Requests
January 1 - June 30, 2018**

Table 2 provides information regarding financial identifier-based requests received. Examples of such requests are where law enforcement agencies are working on behalf of customers who have requested assistance regarding suspected fraudulent credit card activity used to purchase Apple products or services. Financial identifier-based requests generally seek details of suspected fraudulent transactions.

Country or Region	# of Financial Identifier Requests Received	# of Financial Identifiers Specified in the Requests	# of Financial Identifier Requests Where Data Provided	% of Financial Identifier Requests Where Data Provided
Asia Pacific				
Australia	113	1,728	71	63%
China	47	1,662	41	87%
Hong Kong	91	151	65	71%
Japan	73	127	59	81%
Macau	3	6	2	67%
New Zealand	12	42	7	58%
Singapore	35	386	32	91%
South Korea	15	15	12	80%
Taiwan	185	823	163	88%
Asia Pacific Total	574	4,940	452	79%
Europe, Middle East, India, Africa				
Austria	25	351	22	88%
Belgium	14	21	12	86%
Czech Republic	7	7	6	86%
Denmark	2	2	2	100%
Estonia	1	1	1	100%
Finland	1	1	0	0%
France	238	313	165	69%
Germany	1,229	6,389	1,035	84%
Hungary	5	5	4	80%
India	34	3,199	29	85%
Ireland	10	69	3	30%
Italy	129	215	82	64%
Luxembourg	1	1	1	100%
Moldova	2	2	2	100%
Netherlands	1	1	1	100%
Norway	9	10	8	89%
Poland	10	11	10	100%
Portugal	8	9	6	75%
Romania	3	4	3	100%
Russia	5	5	3	60%
Spain	388	399	301	78%
Sweden	8	8	8	100%
Switzerland	139	1,333	94	68%
Turkey	85	88	64	75%
United Arab Emirates	2	2	2	100%
United Kingdom	101	939	80	79%
Europe, Middle East, India, Africa Total	2,457	13,385	1,944	79%
Latin America				
Argentina	2	2	2	100%
Brazil	2	2	2	100%
Chile	1	1	0	0%
Latin America Total	5	5	4	80%
North America				
Canada	18	617	18	100%
Mexico	1	2	0	0%
United States of America	918	14,556	767	84%
North America Total	937	15,175	785	84%
Worldwide Total	3,973	33,505	3,185	80%



of Financial Identifier Requests Received

The number of financial identifier-based requests received from a government agency seeking customer data related to specific financial identifiers, such as credit card or gift card number. Financial identifier-based requests can be in various formats such as subpoenas, court orders, warrants, or other valid legal requests. We count each individual request received from each country/region and report the total number of requests received by country/region.

of Financial Identifiers Specified in the Requests

The number of financial identifiers specified in the requests. One request may contain one or multiple financial identifiers. For example, in a case related to large scale fraud, law enforcement may seek information related to several credit card numbers in a single request. We count the number of financial identifiers identified in each request, received from each country/region, and report the total number of financial identifiers specified in requests received by country/region.

of Financial Identifier Requests Where Data Provided

The number of financial identifier-based requests that resulted in Apple providing data, such as transaction details, in response to a valid legal request. We count each financial identifier-based request where we provide data and report the total number of such instances by country/region.

% of Financial Identifier Requests Where Data Provided

The percentage of financial identifier-based requests that resulted in Apple providing data. We calculate this based on the number of financial identifier-based requests that resulted in Apple providing data per country/region, compared to the total number of financial identifier-based requests Apple received from that country/region.



**Table 3: Worldwide Government Account Requests
January 1 - June 30, 2018**

Table 3 provides information regarding account-based requests received. Examples of such requests are where law enforcement agencies are working on cases where they suspect an account may have been used unlawfully or in violation of Apple's terms of service. Account-based requests generally seek details of customers' iTunes or iCloud accounts, such as a name and address; and in certain instances customers' iCloud content, such as stored photos, email, iOS device backups, contacts or calendars.

Country or Region	# of Account Requests Received	# of Accounts Specified in the Requests	# of Account Requests Challenged in Part or Rejected in Full	# of Account Requests Where Only Non-Content Data Provided	# of Account Requests Where Content Data Provided	% of Account Requests Where Data Provided
Asia Pacific						
Australia	120	140	35	62	1	53%
China	33	19,908	0	32	0	97%
Hong Kong	5	6	0	5	0	100%
Japan	166	320	17	130	0	78%
New Zealand	2	5	0	0	0	0%
Singapore	46	53	2	36	0	78%
South Korea	10	16	0	9	0	90%
Taiwan	241	554	1	200	0	83%
Asia Pacific Total	623	21,002	55	474	1	76%
Europe, Middle East, India, Africa						
Austria	8	18	1	6	0	75%
Belarus	1	110	1	0	0	0%
Belgium	11	19	0	7	0	64%
Czech Republic	3	3	0	3	0	100%
Denmark	1	1	1	0	0	0%
Estonia	1	1	0	1	0	100%
Finland	2	3	0	2	0	100%
France	120	127	9	71	0	59%
Germany	292	393	25	203	2	70%
Greece	10	11	0	9	0	90%
Hungary	4	4	0	2	0	50%
India	18	971	3	14	0	78%
Ireland	5	8	1	2	1	60%
Italy	76	85	12	38	0	50%
Mozambique	1	4	0	1	0	100%
Netherlands	10	16	0	9	0	90%
Norway	6	6	1	3	0	50%
Poland	8	15	0	6	1	88%
Portugal	2	2	2	0	0	0%
Russia	3	3	1	1	0	33%
South Africa	1	1	0	0	0	0%
Spain	43	58	10	21	0	49%
Sweden	7	9	2	5	0	71%
Switzerland	12	20	1	10	0	83%
Turkey	21	24	3	14	0	67%
Ukraine	2	2	0	0	0	0%
United Arab Emirates	1	1	1	0	0	0%
United Kingdom	263	300	28	206	0	78%
Europe, Middle East, India, Africa Total	932	2,215	102	634	4	68%
Latin America						
Argentina	2	2	2	0	0	0%
Brazil	200	980	2	25	150	88%
Chile	3	3	1	2	0	67%
Costa Rica	2	2	0	2	0	100%
Paraguay	1	1	0	1	0	100%
Latin America Total	208	988	5	30	150	87%
North America						
Canada	15	18	0	12	2	93%
Mexico	2	2	0	2	0	100%
United States of America	2,397	16,416	158	1,239	849	87%
North America Total	2,414	16,436	158	1,253	851	87%
Worldwide Total	4,177	40,641	320	2,391	1,006	81%



of Account Requests Received

The number of account-based requests received from a government agency seeking customer data related to specific Apple account identifiers, such as Apple ID or email address. Account-based requests can be in various formats such as subpoenas, court orders, warrants, or other valid legal requests. We count each individual request received from each country/region and report the total number of requests received by country/region.

of Accounts Specified in the Requests

The number of accounts specified in the requests. One request may contain one or multiple account identifiers. For example, in a case related to suspected phishing, law enforcement may seek information related to several accounts in a single request. We count the number of accounts identified in each request, received from each country/region, and report the total number of accounts specified in requests received by country/region.

of Account Requests Challenged in Part or Rejected in Full

The number of account-based requests that resulted in Apple challenging the request in part, or rejecting the request in full, based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate, and/or over-broad. For example, Apple may reject a law enforcement request if it considers the scope of data requested as excessively broad for the case in question. We count each account-based request where we challenge it in part, or reject it in full, and report the total number of such instances by country/region.

of Account Requests Where Only Non-Content Data Provided

The number of account-based requests that resulted in Apple only providing non-content data, such as subscriber, account connections or transactional information, in response to a valid legal request. We count each account-based request where we provide only non-content data and report the total number of such instances by country/region.

of Account Requests Where Content Data Provided

The number of account-based requests that resulted in Apple providing content data, such as stored photos, email, iOS device backups, contacts or calendars, in response to a valid legal request. We count each account-based request where we provide content data and report the total number of such instances by country/region.

% of Account Requests Where Data Provided

The percentage of account-based requests that resulted in Apple providing either non-content and/or content data. We calculate this based on the number of account-based requests that resulted in Apple providing data (including both non-content and content) per country/region, compared to the total number of account-based requests Apple received from that country/region.



**Table 4: Worldwide Government Account Preservation Requests
January 1 - June 30, 2018**

Table 4 provides information regarding account preservation requests received. Under the U.S. Electronic Communications Privacy Act (ECPA) government agencies may request Apple to preserve users' account data by performing a one-time data pull of the requested existing user data available at the time of the request for 90 days (up to 180 days if Apple receives a renewal request). Examples of such requests are where law enforcement agencies suspect an account may have been used unlawfully or in violation of Apple's terms of service, and request Apple to preserve the account data while they obtain legal process for the data.

Country or Region	# of Account Preservation Requests Received	# of Accounts Specified in the Requests	# of Accounts Where Data Preserved
Asia Pacific			
Australia	10	28	11
Asia Pacific Total	10	28	11
Europe, Middle East, India, Africa			
Armenia	2	2	1
Azerbaijan	1	3	1
Belgium	2	2	1
France	1	1	1
Germany	13	15	13
India	1	10	8
Italy	1	3	1
Moldova	1	1	0
Netherlands	1	1	1
Norway	1	1	0
Poland	1	1	1
Sweden	6	16	4
Switzerland	3	3	2
Ukraine	1	1	1
United Kingdom	27	66	52
Europe, Middle East, India, Africa Total	62	126	87
Latin America			
Brazil	2	2	1
Latin America Total	2	2	1
North America			
Canada	11	20	18
United States of America	1,494	3,857	2,685
North America Total	1,505	3,877	2,703
Worldwide Total	1,579	4,033	2,802

of Account Preservation Requests Received

The number of account preservation requests received from a government agency. We count each individual request received from each country/region and report the total number of requests received by country/region.

of Accounts Specified in the Requests

The number of accounts specified in the requests. One request may contain one or multiple account identifiers. For example, in a case related to suspected illegal activity, law enforcement may request Apple to preserve information related to several accounts in a single request. We count the number of accounts identified in each request, received from each country/region, and report the total number of accounts specified in requests received by country/region.

of Accounts Where Data Preserved

The number of accounts that resulted in Apple preserving data in response to a valid preservation request. We count the number of accounts in each request where data was preserved and report the total number of accounts for which data was preserved by country/region.



**Table 5: Worldwide Government Account Restriction/Deletion Requests
January 1 - June 30, 2018**

Table 5 provides information regarding account restriction/deletion requests received. Examples of such requests are where law enforcement agencies suspect an account may have been used unlawfully or in violation of Apple's terms of service, and request Apple to restrict or delete the account. For requests seeking to restrict/delete a customer's Apple ID, Apple requires a court order (including conviction or warrant) demonstrating that the account to be restricted/deleted was used unlawfully.

Country or Region	# of Account Restriction/ Account Deletion Requests Received	# of Accounts Specified in the Requests	# of Requests Rejected/ Challenged Where No Action Taken	# of Account Restriction Requests Where Account Restricted	# of Account Deletion Requests Where Account Deleted
Europe, Middle East, India, Africa					
Switzerland	1	4	0	1	0
Europe, Middle East, India, Africa Total	1	4	0	1	0
North America					
United States of America	4	5	0	2	2
North America Total	4	5	0	2	2
Worldwide Total	5	9	0	3	2

**# of Account
Restriction/Account
Deletion Requests
Received**

The number of requests received from a government agency seeking to restrict or delete a customer's Apple account. We count each individual request received from each country/region and report the total number of requests received by country/region.

**# of Accounts
Specified in the
Requests**

The number of accounts specified in the requests. One request may contain one or multiple account identifiers. For example, in a case related to possession or distribution of illegal material, law enforcement may request Apple to restrict or delete several accounts in a single request. We count the number of accounts identified in each request, received from each country/region, and report the total number of accounts specified in requests received by country/region.

**# of Requests
Rejected/
Challenged Where
No Action Taken**

The number of account restriction/deletion requests that resulted in Apple challenging or rejecting the request based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate, and/or over-broad, or where it is not accompanied by a court order (including conviction or warrant) demonstrating that the account to be restricted/deleted was used unlawfully; and where no action was taken by Apple. We count each account restriction/deletion request where we challenge or reject it and report the total number of such instances by country/region.

**# of Account
Restriction
Requests Where
Account Restricted**

The number of account restriction requests where Apple determined the request and order sufficiently demonstrated the account to be restricted was used unlawfully and we proceeded with the requested restriction. We count each account restriction request where we proceeded with restriction and report the total number of such instances by country/region.

**# of Account
Deletion Requests
Where Account
Deleted**

The number of account deletion requests where Apple determined the request and order sufficiently demonstrated the account to be deleted was used unlawfully and we deleted the Apple account. We count each account deletion request where we deleted an account and report the total number of such instances by country/region.



**Table 6: Worldwide Government Emergency Requests
January 1 - June 30, 2018**

Table 6 provides information regarding emergency requests received. Under the U.S. Electronic Communications Privacy Act (ECPA) government agencies may request Apple to voluntarily disclose information, including customer information and contents of communications, to a government 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. International agencies may make similar requests to Apple under applicable local law. Examples of such requests are where a person may be missing and law enforcement believes the person may be in danger. Emergency requests generally seek details of customers' connections to Apple services.

Country or Region	# of Emergency Requests Received	# of Requests Rejected/Challenged & No Data Provided	# of Emergency Requests Where No Data Provided	# of Emergency Requests Where Data Provided	% of Emergency Requests Where Data Provided
Asia Pacific					
Australia	2	0	1	1	50%
South Korea	1	0	0	1	100%
Taiwan	1	0	0	1	100%
Asia Pacific Total	4	0	1	3	75%
Europe, Middle East, India, Africa					
Czech Republic	1	0	0	1	100%
France	9	0	0	9	100%
Germany	9	0	0	9	100%
Iceland	1	0	0	1	100%
India	3	0	0	3	100%
Ireland	1	0	0	1	100%
Israel	1	0	0	1	100%
Italy	4	0	0	4	100%
Netherlands	2	0	0	2	100%
Norway	3	0	0	3	100%
Poland	2	1	0	1	50%
Slovakia	1	0	0	1	100%
Spain	1	0	0	1	100%
Sweden	1	0	0	1	100%
Switzerland	9	0	3	6	67%
United Arab Emirates	1	0	0	1	100%
United Kingdom	172	0	40	132	77%
Europe, Middle East, India, Africa Total	221	1	43	177	80%
Latin America					
Brazil	3	1	0	2	67%
Dominican Republic	1	0	0	1	100%
Latin America Total	4	1	0	3	75%
North America					
Canada	24	1	1	22	92%
Mexico	9	0	1	8	89%
United States of America	145	6	10	129	89%
North America Total	178	7	12	159	89%
Worldwide Total	407	9	56	342	84%



of Emergency Requests Received

The number of emergency requests received from a government agency. We count each individual request received from each country/region and report the total number of requests received by country/region.

of Requests Rejected/Challenged & No Data Provided

The number of emergency requests that resulted in Apple challenging or rejecting the request based on grounds such as a request is unclear, inappropriate, or fails to demonstrate that it relates to an emergency circumstance; and where no data was provided. We count each emergency request where we challenge or reject it and report the total number of such instances by country/region.

of Emergency Requests Where No Data Provided

The number of emergency requests that resulted in Apple providing no data. For example, instances where there was no responsive data. We count each emergency request where we do not provide data and report the total number of such instances by country/region.

of Emergency Requests Where Data Provided

The number of emergency requests that resulted in Apple providing data, such as connections to Apple services, subscriber or transactional information, in response to a valid emergency request. We count each emergency request where we provide data and report the total number of such instances by country/region.

% of Emergency Requests Where Data Provided

The percentage of emergency requests that resulted in Apple providing data. We calculate this based on the number of emergency requests that resulted in Apple providing data per country/region, compared to the total number of emergency requests Apple received from that country/region.



**Table 7: United States Government National Security Requests
January 1 - June 30, 2018**

Table 7 provides information regarding United States national security requests that Apple received for customer data, including orders received under the Foreign Intelligence Surveillance Act (“FISA”) and National Security Letters (“NSLs”). To date, Apple has not received any orders for bulk data.

We report all national security requests received (NSLs and orders received under FISA) within ranges permissible by law pursuant to the USA FREEDOM Act of 2015 (“USA Freedom”). For Transparency Report Period January 1 - June 30, 2018 and subsequent reports, we have updated the reporting methodology we are utilizing for national security reporting. In order to report FISA non-content and content requests in separate categories, Apple is required by law to delay reporting by 6 months and report in bands of 500. Though we want to be more specific, this is currently the range permitted under USA Freedom for reporting this level of detail regarding national security requests.

National Security Request Type	# of Requests Received	# of Users/Accounts
FISA Non-Content Requests	0 - 499	7,500 - 7,999
FISA Content Requests	0 - 499	13,500 - 13,999
National Security Letters	0 - 499	1,000 - 1,499
National Security Letters where non-disclosure order lifted	0	

National Security Request Type

FISA Non-Content & Content Requests: FISA Court issued orders for non-content or content data. Non-content data is data such as subscriber or transactional information and connection logs. Content data is data such as stored photos, email, iOS device backups, contacts or calendars.

National Security Letters: Federal Bureau of Investigation issued requests for non-content data in national security investigations. Non-content data is data such as subscriber data. Apple does not produce transactional information and connection logs in response to National Security Letters.

of Requests Received

The number of United States National Security requests received. We count each individual order and National Security Letter received and report the total number of orders and National Security Letters received within bands permissible by law. Pursuant to USA Freedom, to report the number of non-content and content orders received, we are limited to providing this data in bands of 500.

of Users/Accounts

We count the number of users/accounts in each request received for which Apple has data and report the total number of users/accounts within bands permissible by law. Pursuant to USA Freedom, we are limited to providing this data in bands of 500.

National Security Letters where non-disclosure order lifted

The number of National Security letters Apple received where the non-disclosure order has been lifted during the current transparency reporting period.



**Tables 8, 9, 10: United States Government Requests by Legal Process Type
January 1 - June 30, 2018**

Tables 8, 9, and 10 provide information regarding United States requests by legal process type. Legal process types can be Search Warrants, Wiretap Orders, Pen Register/Trap and Trace Orders, Other Court Orders, or Subpoenas.

Table 8: United States Government Device Requests by Legal Process Type

Table 8 provides information regarding the types of legal process Apple received as Device Requests.

# of Device Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
4,570	333	N/A	1	193	4,043
% of Total (100%)	7%	-	~0%	4%	88%

Table 9: United States Government Financial Identifier Requests by Legal Process Type

Table 9 provides information regarding the types of legal process Apple received as Financial Identifier Requests.

# of Financial Identifier Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
918	133	N/A	0	59	726
% of Total (100%)	14%	-	0%	6%	79%

Table 10: United States Government Account Requests by Legal Process Type

Table 10 provides information regarding the types of legal process Apple received as Account Requests.

# of Account Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
2,397	963	0	34	191	1,209
% of Total (100%)	40%	0%	1%	8%	50%



of Device/ Financial Identifier/ Account Requests

The total number of United States government requests Apple received by request type (Device, Financial Identifier, and Account). We count each individual request received from the United States by request type and report the total number of requests received by request type.

Search Warrants

A search warrant is a judicial document used in a criminal case authorizing law enforcement officers to search a person or place to obtain evidence. The Fourth Amendment requires that law enforcement officers obtain search warrants by submitting affidavits and other evidence to a judge or magistrate to meet a burden of proof that a search will yield evidence related to a crime. The judge or magistrate will issue the warrant if satisfied that the law enforcement officers have met the burden of proof. For customer content, Apple requires a search warrant issued upon a showing of probable cause in order to provide content.

Wiretap Orders

A wiretap order is a specific type of court order used in a criminal case that authorizes law enforcement officers to obtain contents of communications in real-time. A Title III wiretap order includes requirements that law enforcement officers make an application and furnish evidence to a judge or magistrate to demonstrate there is probable cause to believe that interception of communications will yield evidence related to a particular crime, there is probable cause to believe that an individual has committed or is about to commit a particular crime and must specifically identify the individual/target whose communications are to be intercepted. A statement must also be included as to whether other investigatory measures have been tried and failed or are unlikely to succeed. If satisfied that the requirements have been met, the judge or magistrate will issue the wiretap order. A wiretap order allows the government to obtain content on a forward-looking basis for a specific limited period of time as opposed to stored historical content. Apple can intercept users' iCloud email communications upon receipt of a valid Wiretap Order. Apple cannot intercept users' iMessage or FaceTime communications as these communications are end-to-end encrypted.

Pen Register/Trap & Trace Orders

A pen register or trap and trace order is a specific type of court order used in a criminal case authorizing law enforcement officers to obtain headers of electronic communications and other non-content data in real-time. A pen register order requires law enforcement officers to make a statement of offense which the pen register relates and certify the information likely to be obtained is relevant/material to an ongoing criminal investigation. The legal standard for obtaining a pen register order is lower than what is required for a search warrant or a wiretap order. A pen register order allows the government to obtain non-content data on a forward-looking basis for a specific limited period of time as opposed to stored historical information. A pen register order can be combined with a court order/warrant for historical records, in such instances we report the process type as pen register/trap and trace order.

Other Court Orders

A court order is a document issued by a judge or magistrate directing a person or entity to comply with the order. An order may be issued in either a criminal or civil case. Government agencies applying for an order in a criminal case must generally present facts and evidence to a judge or magistrate showing there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation or similar legal standard. Non-content data such as subscriber and transaction information can be provided in response to a court order.

Subpoenas

A subpoena or equivalent legal process request (e.g. petition or summons) is a document issued by a government agency or court directing a person or entity to comply with requests for information. Local, state and federal government agencies may issue subpoenas. Under many jurisdictions, a judge or magistrate is not required to review a subpoena before it is issued. Accordingly, the subpoena has the lowest threshold for burden of proof. A subpoena may be issued in either a criminal or civil case. Non-content data such as device, subscriber and connection information can be provided in response to a subpoena.

% of Total

The percentage of requests by Legal Process Type. We calculate this based on the number of respective Legal Process Types compared to the respective total number of Device/Financial Identifier/Account Requests received by Apple.



**Table 11: United States Private Party Requests for Information
January 1 - June 30, 2018**

Table 11 provides information regarding United States private party (non-government) requests for information. Examples of such requests are where private litigants are involved in either civil or criminal proceedings. Apple complies with these requests insofar as we are legally required to do so.

# of Private Party Requests	# of Requests Rejected/ Challenged & No Data Provided	# of Requests Where No Data Provided	# of Requests Where Data Provided
215	142	21	52
% of Total (100%)	66%	10%	24%

- # of Private Party Requests** The number of requests received from private parties (non-government) in the United States seeking customer data related to specific devices, financial identifiers and/or accounts. We count each individual request received from private parties and report the total number of requests received.
- # of Requests Rejected/Challenged & No Data Provided** The number of private party requests that resulted in Apple challenging or rejecting the request based on grounds such as a request does not have a valid legal basis, or is unclear and/or over-broad; and where no data was provided. We count each private party request where we challenge or reject it in full, and report the total number of such instances.
- # of Requests Where No Data Provided** The number of private party requests that resulted in Apple providing no data. For example, where there was no responsive data. We count each instance where we do not provide data in response to a private party request and report the total number of such instances.
- # of Requests Where Data Provided** The number of private party requests that resulted in Apple providing data in response to valid legal process or subscriber consent. We count each instance where we provide data in response to a private party request and report the total number of such instances.
- % of Total** The percentages are calculated based on the number of the respective response types compared to the total number of private party requests received by Apple.



**Table 12: United States Private Party Requests for Account Restriction/Deletion
January 1 - June 30, 2018**

Table 12 provides information regarding United States private party (non-government) requests for Apple account restriction/deletion. Examples of such requests are where private litigants are involved in either civil or criminal proceedings, and requests for Apple to restrict/delete an account may arise. For requests seeking to restrict/delete a customer’s Apple ID, Apple requires a court order. Apple complies with these requests insofar as we are legally required to do so.

# of Account Restriction/ Account Deletion Requests Received	# of Accounts Specified in the Requests	# of Requests Rejected/ Challenged Where No Action Taken	# of Account Restriction Requests Where Account Restricted	# of Account Deletion Requests Where Account Deleted
0	0	0	0	0

**# of Account
Restriction/Account
Deletion Requests
Received**

The number of requests received from private parties (non-government), such as participants in a civil or family law case, seeking to restrict or delete a customer’s Apple ID. We count each individual request received from private parties and report the total number of requests received.

**# of Accounts
Specified in the
Requests**

The number of accounts specified in the requests. One request may contain one or multiple account identifiers. For example, in a case related to multiple shared accounts, a private party may request Apple to restrict or delete several accounts in a single request. We count the number of accounts identified in each request received from private parties and report the total number of accounts specified in requests received.

**# of Requests
Rejected/Challenged
Where No Action
Taken**

The number of account restriction/deletion requests that resulted in Apple challenging or rejecting the request based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate, and/or over-broad, or where it is not accompanied by a court order demonstrating the grounds upon which the account is to be restricted/deleted; and where no action was taken by Apple. We count each account restriction/deletion request where we challenge or reject it and report the total number of such instances.

**# of Account
Restriction Requests
Where Account
Restricted**

The number of account restriction requests where Apple determined the request and order sufficiently demonstrated the grounds upon which the specified account was to be restricted; and we proceeded with the requested restriction. We count each account restriction request where we proceeded with restriction and report the total number of such instances.

**# of Account
Deletion Requests
Where Account
Deleted**

The number of account deletion requests where Apple determined the request and order sufficiently demonstrated the grounds upon which the specified account was to be deleted; and we deleted the Apple account. We count each account deletion request where we deleted an account and report the total number of such instances.



Matters of note in this report

Table 1 Worldwide Government Device Requests

China - High number of devices specified in requests predominantly due to insurance fraud and stolen device investigations.

Finland - High number of devices specified in requests due to a stolen device investigation.

Germany - High volume of device requests predominantly due to stolen devices investigations.

Poland - High number of devices specified in requests predominantly due to tax fraud investigations from Customs and Revenue Authorities.

South Korea - High number of devices specified in requests predominantly due to stolen device investigations.

Table 2 Worldwide Government Financial Identifier Requests

Australia - High number of financial identifiers specified in requests predominantly due to iTunes Gift Card and credit card fraud investigations.

Canada - High number of financial identifiers specified in requests predominantly due to iTunes Gift Card and credit card fraud investigations.

China - High number of financial identifiers specified in requests predominantly due to iTunes Gift Card investigations.

Germany - High number of financial identifier requests predominantly due to iTunes Gift Card and credit card fraud investigations.

India - High number of financial identifiers specified in requests predominantly due to an iTunes Gift Card fraud investigation.

United States - High number of financial identifier requests predominantly due to iTunes Gift Card and credit card fraud investigations. High number of financial identifiers specified in requests predominantly due to Reseller fraud, iTunes Gift Card fraud, and financial fraud investigations.

Table 3 Worldwide Government Account Requests

Brazil - High number of accounts specified in court orders; investigation type was not indicated in these orders.

China - High number of accounts specified in requests predominantly due to a fraud investigation.

India - High number of accounts specified in requests predominantly due to an iTunes Gift Card fraud investigation.

United States - High number of accounts specified in requests predominantly due to extortion, fraud, and suspected unauthorized account access/phishing investigations.

Mutual Legal Assistance Treaty (MLAT) Requests

Requests received from a foreign government pursuant to the MLAT process or through other cooperative efforts with the United States government are included in Apple's transparency report. Apple has been able to determine 14 MLAT requests for information were issued by the United States government in this reporting period. However, this may not be the precise number of MLAT requests received, as in some instances a United States court order or search warrant may not indicate that it is the result of an MLAT request. In instances where the originating country was identified, we count and report the MLAT request under the country of origin. In instances where the originating country was not identified, we count and report the request under the United States of America.

Matters of note for future reports

Starting with the Transparency Report period July 1 - December 31, 2018, Apple will report on Government requests to take down Apps from the App Store in instances related to alleged violations of legal and/or policy provisions.