

Apple Transparency Report: Government and Private Party Requests

July 1 - December 31, 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 July 1 through December 31, 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), Auskunftsersuchen (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
- 13) Worldwide Government App Store Takedown Requests - Legal Violations
- 14) Worldwide Government App Store Takedown Requests - Platform Policy Violations

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
July 1 - December 31, 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 ¹	# 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	1,817	2,648	1,369	75%
China mainland	689	137,595	660	96%
Hong Kong	320	545	274	86%
Japan	754	2,386	603	80%
Macau	4	6	3	75%
Malaysia	2	4	1	50%
New Zealand	335	409	289	86%
Philippines	1	2	0	0%
Singapore	1,682	1,719	1,348	80%
South Korea	50	4,105	28	56%
Taiwan	93	205	76	82%
Thailand	2	3	1	50%
Asia Pacific Total	5,749	149,627	4,652	81%
Europe, Middle East, India, Africa				
Andorra	22	27	18	82%
Austria	418	620	266	64%
Belgium	171	394	158	92%
Croatia	1	1	1	100%
Cyprus	1	3	0	0%
Czech Republic	31	47	24	77%
Denmark	121	154	90	74%
Finland	3	10	1	33%
France	943	1,742	715	76%
Germany	12,343	19,380	9,548	77%
Greece	25	43	15	60%
Hungary	38	85	30	79%
India	49	267	23	47%
Ireland	95	163	75	79%
Israel	1	4	1	100%
Italy	414	836	258	62%
Liechtenstein	2	2	1	50%
Luxembourg	7	36	5	71%
Netherlands	28	88	13	46%
Norway	17	21	11	65%
Poland	30	1,702	24	80%
Portugal	139	157	87	63%
Romania	6	6	4	67%
Russia	579	7,264	403	70%
Slovenia	10	110	8	80%
South Africa	14	334	13	93%
Spain	1,736	3,126	1,352	78%
Sweden	92	136	75	82%
Switzerland	288	709	179	62%
Turkey	39	58	20	51%
United Arab Emirates	1	3	1	100%
United Kingdom	541	1,426	435	80%
Europe, Middle East, India, Africa Total	18,205	38,954	13,854	76%
Latin America				
Argentina	3	64	1	33%
Brazil	491	5,675	367	75%
Chile	33	35	23	70%
Colombia	3	23	1	33%
Dominican Republic	1	4	0	0%
Nicaragua	1	1	1	100%
Paraguay	1	1	0	0%
Latin America Total	533	5,803	393	74%
North America				
Canada	16	35	14	88%
United States of America	4,680	19,318	3,778	81%
North America Total	4,696	19,353	3,792	81%
Worldwide Total	29,183	213,737	22,691	78%

¹ Only countries / regions where Apple received device requests during the report period of July 1 - December 31, 2018, are listed.



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
July 1 - December 31, 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 ¹	# 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	110	814	61	55%
China mainland	95	471	83	87%
Hong Kong	200	282	97	49%
Japan	136	334	101	74%
Macau	32	68	26	81%
New Zealand	5	6	1	20%
Singapore	35	160	31	89%
South Korea	36	39	23	64%
Taiwan	298	616	279	94%
Thailand	1	1	0	0%
Asia Pacific Total	948	2,791	702	74%
Europe, Middle East, India, Africa				
Austria	19	288	9	47%
Belgium	26	75	23	88%
Czech Republic	9	9	5	56%
Denmark	1	1	0	0%
France	199	778	156	78%
Germany	1,327	4,890	1,128	85%
Hungary	2	2	2	100%
India	28	28	16	57%
Ireland	10	128	6	60%
Italy	128	135	25	20%
Luxembourg	2	2	2	100%
Monaco	1	1	1	100%
Netherlands	4	4	3	75%
Norway	10	10	3	30%
Poland	19	29	9	47%
Portugal	3	3	2	67%
Romania	3	3	3	100%
Russia	4	4	1	25%
Spain	629	674	420	67%
Sweden	5	5	4	80%
Switzerland	106	979	77	73%
Turkey	79	79	55	70%
United Arab Emirates	1	1	0	0%
United Kingdom	77	971	66	86%
Europe, Middle East, India, Africa Total	2,692	9,099	2,016	75%
Latin America				
Argentina	1	1	0	0%
Brazil	8	14	4	50%
Chile	1	1	0	0%
Costa Rica	4	4	0	0%
Latin America Total	14	20	4	29%
North America				
Canada	11	840	10	91%
Mexico	1	1	0	0%
United States of America	960	8,283	815	85%
North America Total	972	9,124	825	85%
Worldwide Total	4,626	21,034	3,547	77%

¹ Only countries / regions where Apple received financial identifier requests during the report period of July 1 - December 31, 2018, are listed.



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
July 1 - December 31, 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 ¹	# 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	114	154	40	66	0	58%
China mainland	42	7,154	0	38	3	98%
Hong Kong	8	8	3	3	0	38%
Japan	249	351	42	188	0	76%
New Zealand	15	27	2	13	0	87%
Singapore	34	43	1	26	0	76%
South Korea	13	13	5	8	0	62%
Taiwan	370	883	1	328	0	89%
Asia Pacific Total	845	8,633	94	670	3	80%
Europe, Middle East, India, Africa						
Andorra	1	1	1	0	0	0%
Austria	6	11	3	3	0	50%
Belgium	9	14	0	9	0	100%
Czech Republic	8	11	2	6	0	75%
Denmark	1	1	1	0	0	0%
Estonia	1	1	0	1	0	100%
Finland	2	2	0	2	0	100%
France	154	177	12	98	1	64%
Germany	335	417	28	241	2	73%
Greece	4	5	1	2	0	50%
Hungary	2	2	0	2	0	100%
India	18	18	5	11	0	61%
Ireland	5	30	0	3	0	60%
Italy	48	60	31	18	0	38%
Malta	2	2	0	1	0	50%
Netherlands	14	17	2	11	0	79%
Norway	3	3	3	0	0	0%
Poland	12	15	5	4	0	33%
Portugal	4	4	3	1	0	25%
Russia	13	21	6	5	0	38%
Spain	48	88	15	24	0	50%
Sweden	33	47	0	27	1	85%
Switzerland	19	24	2	12	1	68%
Turkey	20	26	2	15	0	75%
United Kingdom	293	395	31	234	1	80%
Europe, Middle East, India, Africa Total	1,055	1,392	153	730	6	70%
Latin America						
Argentina	1	1	0	1	0	100%
Brazil	294	2,529	10	36	213	85%
Chile	1	1	1	0	0	0%
Colombia	1	1	1	0	0	0%
Dominican Republic	1	2	1	0	0	0%
Paraguay	1	1	0	0	0	0%
Latin America Total	299	2,535	13	37	213	84%
North America						
Canada	7	19	1	6	0	86%
United States of America	2,669	9,924	102	1,339	1,005	88%
North America Total	2,676	9,943	103	1,345	1,005	88%
Worldwide Total	4,875	22,503	363	2,782	1,227	82%

¹ Only countries / regions where Apple received account requests during the report period of July 1 - December 31, 2018, are listed.



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
July 1 - December 31, 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 ¹	# of Account Preservation Requests Received	# of Accounts Specified in the Requests	# of Accounts Where Data Preserved
Asia Pacific			
Australia	6	12	4
New Zealand	2	5	2
Asia Pacific Total	8	17	6
Europe, Middle East, India, Africa			
Armenia	1	1	0
Belarus	2	6	2
Finland	1	1	1
France	3	5	5
Germany	5	9	6
India	3	4	1
Ireland	1	2	1
Italy	1	1	1
Luxembourg	2	2	1
Netherlands	4	6	5
Norway	2	2	2
Poland	1	1	0
Portugal	1	1	1
Sweden	10	11	11
Switzerland	1	6	6
Ukraine	1	1	1
United Kingdom	32	50	47
Europe, Middle East, India, Africa Total	71	109	91
Latin America			
Argentina	2	5	5
Brazil	7	9	8
Venezuela	1	1	0
Latin America Total	10	15	13
North America			
Canada	10	66	64
United States of America	1,724	5,346	3,789
North America Total	1,734	5,412	3,853
Worldwide Total	1,823	5,553	3,963

¹ Only countries / regions where Apple received account preservation requests during the report period of July 1 - December 31, 2018, are listed.

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
July 1 - December 31, 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 ¹	# 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
Asia Pacific					
Hong Kong	1	1	1	0	0
Japan	1	1	1	0	0
Asia Pacific Total	2	2	2	0	0
Europe, Middle East, India, Africa					
Denmark	1	1	1	0	0
Germany	2	2	2	0	0
India	1	1	1	0	0
Italy	1	1	1	0	0
United Kingdom	2	2	0	0	0
Europe, Middle East, India, Africa Total	7	7	5	0	0
North America					
United States of America	6	13	1	2	2
North America Total	6	13	1	2	2
Worldwide Total	15	22	8	2	2

¹ Only countries / regions where Apple received account restriction/deletion requests during the report period of July 1 - December 31, 2018, are listed.

**# 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
July 1 - December 31, 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 ¹	# 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	3	1	0	2	67%
Japan	10	0	1	9	90%
New Zealand	1	0	0	1	100%
Singapore	2	0	0	2	100%
Asia Pacific Total	16	1	1	14	88%
Europe, Middle East, India, Africa					
Austria	2	0	0	2	100%
Belgium	2	0	0	2	100%
Czech Republic	1	0	0	1	100%
Denmark	1	0	0	1	100%
France	11	0	0	11	100%
Germany	16	1	0	15	94%
India	8	0	2	6	75%
Israel	1	0	0	1	100%
Italy	3	0	0	3	100%
Kosovo	1	0	0	1	100%
Netherlands	6	0	1	5	83%
Norway	3	0	0	3	100%
Qatar	1	1	0	0	0%
Sweden	1	0	0	1	100%
Switzerland	6	0	1	5	83%
Ukraine	1	0	0	1	100%
United Kingdom	198	0	25	173	87%
Europe, Middle East, India, Africa Total	262	2	29	231	88%
Latin America					
Brazil	5	1	1	3	60%
Latin America Total	5	1	1	3	60%
North America					
Canada	17	0	0	17	100%
Mexico	5	1	0	4	80%
United States of America	189	1	10	178	94%
North America Total	211	2	10	199	94%
Worldwide Total	494	6	41	447	90%

¹ Only countries / regions where Apple received emergency requests during the report period of July 1 - December 31, 2018, are listed.



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
July 1 - December 31, 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"). 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	9,000 - 9,499
FISA Content Requests	0 - 499	14,000 - 14,499
National Security Letters	3 - 499	1,505 - 1,999

The below table shows the three National Security Letters received during this reporting period where the non-disclosure orders have been lifted and public disclosure is permitted. In addition, this table includes a complete historical list of National Security Letters received to date where the non-disclosure orders have been lifted and public disclosure is permitted. See [Apple's Transparency website](#) for redacted PDFs of these National Security Letters.

National Security Letter #	Issue Date	Non-Disclosure Order End Date
NSL-18-466228	12/27/18	5/5/19
NSL-18-463687	12/6/18	5/5/19
NSL-18-450995	8/28/18	5/6/19
NSL-18-440748	3/15/18	4/9/19
NSL-15-413741	4/8/15	2/25/17

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 Letter #

Government-issued reference number assigned when a National Security Letter is approved and signed by a Federal Bureau of Investigation Special Agent in Charge.

Issue Date

Date the National Security Letter was approved and signed by the Special Agent in Charge.

Non-Disclosure Order End Date

Date where a non-disclosure order for a specific National Security Letter is lifted and public disclosure of the National Security Letter is permitted.



**Tables 8, 9, 10: United States Government Requests by Legal Process Type
July 1 - December 31, 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
4,680	381	N/A	3	151	4,145
% of Total (100%)	8%	-	~0%	3%	89%

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
960	113	N/A	0	55	792
% of Total (100%)	12%	-	0%	6%	82%

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
2,669	1,119	0	26	237	1,287
% of Total (100%)	42%	0%	1%	9%	48%



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
July 1 - December 31, 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
181	110	18	53
% of Total (100%)	61%	10%	29%

- # 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
July 1 - December 31, 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
1	1	1	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.



**Table 13: Worldwide Government App Store Takedown Requests - Legal Violations
July 1 - December 31, 2018**

Table 13 provides information regarding requests from government authorities to remove apps from the App Store based on alleged/suspected violations of local law. Examples of such requests are where law enforcement or regulatory agencies suspect an app may be unlawful or relate to/contain unlawful content. Apple complies with these requests insofar as we are legally required to do so.

Country or Region ¹	# of Legal Violation Takedown Requests Received	# of Apps Specified in the Requests	# of Requests Challenged in Part or Rejected in Full	# of Requests Where App Removed	# of Apps Removed
Asia Pacific					
China mainland ²	56	626	2	55	517
Vietnam ³	3	29	3	1	9
Asia Pacific Total	59	655	5	56	526
Europe, Middle East, India, Africa					
Austria ⁴	1	5	0	1	5
Kuwait ⁵	1	6	1	1	5
Lebanon ⁵	1	1	0	1	1
Netherlands ⁴	2	8	0	2	8
Norway ⁴	1	37	0	1	37
Russia ⁴	10	11	0	9	10
Saudi Arabia ⁵	1	25	0	1	25
Switzerland ⁴	1	19	0	1	15
Turkey ⁶	3	3	1	2	2
Europe, Middle East, India, Africa Total	21	115	2	19	108
Worldwide Total	80	770	7	75	634

¹ Only countries / regions where Apple received legal violation removal requests during the report period of July 1 - December 31, 2018, are listed.

² The vast majority relate to illegal gambling or pornography.

³ Requests relate to illegal gambling and/or unlicensed gaming app investigations.

⁴ All or vast majority of requests relate to illegal gambling investigations.

⁵ Requests relate to violations of privacy law.

⁶ Requests relate to copyright infringement, illegal content, and violation of local transportation law.

of Legal Violation Takedown Requests Received

The number of requests received from a government agency seeking to take down a third party application offered on the App Store related to alleged/suspected legal violations. We count each individual request received from each country or region and report the total number of requests received by country or region.

of Apps Specified in the Requests

The number of apps specified in the requests verified to be apps available on the App Store. One request may contain one or multiple apps. A government agency may request Apple to take down several apps in a single request. We count the number of apps identified in each request received from each country or region and report the total number of apps specified in requests received by country or region.

of Requests Challenged in Part or Rejected in Full

The number of app takedown requests related to alleged/suspected legal violations that resulted in Apple challenging or rejecting the request in part or in full based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate and/or over-broad, or does not sufficiently demonstrate the legal violation of the app to be removed. We count each App Store takedown request related to alleged/suspected legal violations where we challenge or reject it in part or in full and report the total number of such instances by country or region.

of Requests Where App Removed

The number of App Store takedown requests where the request sufficiently demonstrated a valid legal violation and Apple proceeded with removal of app(s) from the App Store. We count each app takedown request related to alleged/suspected legal violations where we proceeded with app removal and report the total number of such instances by country or region.

of Apps Removed

The number of App Store takedown requests where the request sufficiently demonstrated a valid legal violation and Apple proceeded with removal of app(s) from the App Store. We count each app takedown request related to alleged/suspected legal violations where we proceeded with app removal and report the total number of apps removed in such instances by country or region.



**Table 14: Worldwide Government App Store Takedown Requests - Platform Policy Violations
July 1 - December 31, 2018**

Table 14 provides information regarding requests from government authorities to remove apps from the App Store based on alleged/suspected violations of App Store platform policies. Examples of such requests are where law enforcement or regulatory agencies suspect an app may violate the App Store platform policies or relate to/contain content violating platform policies. Apple complies with these requests where Apple has determined there is an App Store platform policy violation.

Country or Region ¹	# of Platform Policy Violation Takedown Requests Received	# of Apps Specified in the Requests	# of Requests Challenged in Part or Rejected in Full	# of Requests Where App Removed	# of Apps Removed
N/A	0	0	0	0	0

¹ Only countries / regions where Apple received platform violation removal requests during the report period of July 1 - December 31, 2018, are listed.

of Platform Policy Violation Takedown Requests Received

The number of requests received from a government agency seeking to take down a third party application offered on the App Store related to alleged/suspected platform policy violations. We count each individual request received from each country or region and report the total number of requests received by country or region.

of Apps Specified in the Requests

The number of apps specified in the requests verified to be apps available on the App Store. One request may contain one or multiple apps. A government agency may request Apple to take down several apps in a single request. We count the number of apps identified in each request received from each country or region and report the total number of apps specified in requests received by country or region.

of Requests Challenged in Part or Rejected in Full

The number of app takedown requests related to alleged/suspected platform policy violations that resulted in Apple challenging or rejecting the request in part or in full based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate and/or over-broad, or does not sufficiently demonstrate the platform policy violation of the app to be removed. We count each App Store takedown request related to alleged/suspected platform policy violations where we challenge or reject it in part or in full and report the total number of such instances by country or region.

of Requests Where App Removed

The number of App Store takedown requests where Apple determined the request sufficiently demonstrated a valid App Store platform policy violation and Apple proceeded with removal of app(s) from the App Store. We count each app takedown request related to alleged/suspected platform policy violations where we proceeded with app removal and report the total number of such instances by country or region.

of Apps Removed

The number of App Store takedown requests where Apple determined the request sufficiently demonstrated a valid App Store platform policy violation and Apple proceeded with removal of app(s) from the App Store. We count each app takedown request related to alleged/suspected platform policy violations where we proceeded with app removal and report the total number of apps removed in such instances by country or region.



Matters of note in this report:

Government requests related to customer data / accounts

Table 1 Worldwide Government Device Requests

Brazil - High number of devices specified due to a stolen device investigation.

China mainland - High number of devices specified in requests predominantly due to tax fraud investigations from Taxation Administration Authorities.

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

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

Russia - High number of devices specified in requests predominantly due to a Customs fraud investigation.

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

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

Table 2 Worldwide Government Financial Identifier Requests

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

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

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

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

Table 3 Worldwide Government Account Requests

Brazil - High number of accounts specified in requests predominantly due to financial fraud investigations.

China mainland - High number of accounts specified in requests predominantly due to financial fraud investigations.

Table 5 Worldwide Government Account Restriction/Deletion Requests

United Kingdom - Apple had no relevant accounts for the information provided in account restriction/deletion requests.

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 8 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 in this report:

Government requests related to app removals

Table 13 Worldwide Government App Store Takedown Requests - Legal Violations

Austria - Request related to illegal gambling app investigations.

China mainland - The vast majority relate to illegal gambling or pornography.

Kuwait - Request related to investigation of apps with suspected violation of privacy law.

Lebanon - Request related to investigation of app with suspected violation of privacy law.

Netherlands - Requests related to illegal gambling app investigations.

Norway - Request related to illegal gambling app investigations.

Russia - Requests predominantly related to illegal gambling app investigations.

Saudi Arabia - Request related to investigation of apps with suspected violation of privacy law.

Switzerland - Request related to illegal gambling app investigations.

Turkey - Requests related to investigation of illegal app content, including breach of copyright and suspected violation of local transportation law.

Vietnam - Requests predominantly related to illegal gambling app investigations and unlicensed gaming apps investigations.

Matters of note for future reports

In addition to reporting on Government requests to remove Apps from the App Store in instances related to alleged violations of legal and/or policy provisions, starting with the Transparency Report period July 1 - December 31, 2019, Apple will report on appeals received pursuant to such Government requests.