Apple Transparency Report: Government and Private Party Requests

July 1 - December 31, 2019

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, 2019.

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, 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.

The restrictions imposed by the sanctions laws generally prohibit Apple from responding to requests from countries, territories or governments sanctioned by the U.S. Department of Treasury, with the exception of requests involving exempt informational material or where prior authorization has been secured.

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, 2019

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	1,694	3,015	1,089	64%
China mainland	781	22,187	756	97%
Hong Kong	246	271	160	65%
Japan	1,245	3,882	1,105	89%
Macau	1	1	1	100%
New Zealand	208	219	124	60%
Singapore	1,324	1,349	1,197	90%
South Korea	45	6,292	24	53%
Taiwan	144	361	102	71%
Thailand	12	29	1	8%
Asia Pacific Total	5,700	37,606	4,559	80%
Europe, Middle East, India, Africa				
Andorra	18	21	16	89%
Austria	400	620	202	51%
Belgium	108	198	88	81%
Czech Republic	62	555	44	71%
Denmark	48	62	38	79%
Estonia	1	1	1	100%
Finland	2	3	1	50%
France	789	1,563	530	67%
Germany	13,761	21,371	10,986	80%
Greece	64	71	56	88%
Hungary	39	47	32	82%
India	42	126	21	50%
Ireland	112	224	90	80%
Italy	320	603	124	39%
Kenya	1	2	0	0%
Liechtenstein	1	1	0	0%
Luxembourg	8	34	8	100%
Malta	1	1	1	100%
Monaco	1	1	0	0%
Netherlands	37	117	27	73%
North Macedonia	1	1	0	0%
Norway	22	47	8	36%
Poland	46	2,543	34	74%
Portugal	113	129	73	65%
Romania	7	10	4	57%
Russia	973	1,499	816	84%
Slovakia	2	4	0	0%
Slovenia	15	81	15	100%
South Africa	7	370	7	100%
Spain	1,491	2,695	1,204	81%
Sweden	92	950	86	93%
Switzerland	225	511	183	81%
Turkey	43	52	16	37%
United Arab Emirates	1	1	1	100%
United Kingdom	568	1,223	392	69%
Europe, Middle East, India, Africa Total	19,421	35,737	15,104	78%
Latin America				
Brazil	1,098	4,614	929	85%
Chile	51	707	44	86%
Colombia	1	1	1	100%
Latin America Total	1,150	5,322	974	85%
North America				
Canada	24	228	22	92%
United States of America	5,271	80,235	4,396	83%
North America Total	5,295	80,463	4,418	83%
Worldwide Total	31,566	159,128	25,055	79%

[1] Only countries / regions where Apple received device requests during report period July 1 - December 31, 2019, 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, 2019

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	83	678	52	63%
China mainland	26	55	21	81%
Hong Kong	155	230	54	35%
Japan	173	5,620	144	83%
Macau	6	6	3	50%
New Zealand	2	3	1	50%
Singapore	89	711	73	82%
South Korea	24	57	15	63%
Taiwan	319	361	302	95%
Thailand	1	1	0	0%
Asia Pacific Total	878	7,722	665	76%
Europe, Middle East, India, Africa				
Austria	28	141	2	7%
Belgium	12	141	10	83%
Bulgaria	1	1	0	0%
Czech Republic	11	12	10	91%
Denmark	6	6	2	33%
Estonia	1	1	1	100%
Finland	6	71	1	17%
France	401	1,118	244	61%
Germany	786	4,823	693	88%
Greece	1	1	0	0%
Hungary	7	8	5	71%
India	211	247	108	51%
Ireland	12	129	9	75%
Israel	1	1	1	100%
Italy	118	163	21	18%
Liechtenstein	1	1	1	100%
Lithuania	1	1	0	0%
Luxembourg	1	1	1	100%
Netherlands	3	3	3	100%
Norway	5	5	4	80%
Poland	41	42	32	78%
Portugal	19	49	14	74%
Qatar	1	1	0	0%
Romania	23	23	21	91%
Russia	32	40	11	34%
Slovenia	2	2	0	0%
Spain	711	845	488	69%
Sweden	3	3	3	100%
Switzerland	70	764	55	79%
Turkey	193	196	126	65%
United Arab Emirates	3	3	1	33%
United Kingdom	41	880	25	61%
Europe, Middle East, India, Africa Total	2,752	9,722	1,892	69%
Latin America				
Argentina	1	4	1	100%
Brazil	5	5	3	60%
Costa Rica	3	3	2	67%
Latin America Total	9	12	6	67%
North America				
Canada	5	6	3	60%
Mexico	1	3	1	100%
United States of America	582	3,399	425	73%
North America Total	588	3,408	429	73%
Worldwide Total	4,227	20,864	2,992	71%

[1] Only countries / regions where Apple received financial identifier requests during report period July 1 - December 31, 2019, 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, 2019

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	142	181	14	106	1	75%
China mainland	45	2,085	0	39	2	91%
Hong Kong	8	12	1	3	0	38%
Japan	309	475	27	263	0	85%
New Zealand	8	13	2	3	0	38%
Singapore	45	47	1	38	0	84%
South Korea	25	32	12	11	0	44%
Taiwan	492	966	2	421	0	86%
Asia Pacific Total	1,074	3,811	59	884	3	83%
Europe, Middle East, India, Africa						
Andorra	2	3	0	2	0	100%
Austria	13	19	5	2	1	23%
Belgium	13	35	0	12	0	92%
Czech Republic	12	17	1	9	0	75%
Denmark	4	9	2	1	1	50%
Finland	4	10	3	1	0	25%
France	250	356	38	145	1	58%
Germany	480	696	38	366	0	76%
Greece	5	5	0	4	0	80%
Hungary	5	17	0	5	0	100%
India	12	15	6	6	0	50%
Ireland	10	25	2	7	1	80%
Italy	42	44	24	13	0	31%
Kuwait	1	1	1	0	0	0%
Latvia	1	1	1	0	0	0%
Malta	1	1	0	1	0	100%
Moldova	2	2	1	1	0	50%
Monaco	1	1	1	0	0	0%
Netherlands	69	204	5	36	1	54%
North Macedonia	1	1	1	0	0	0%
Norway	5	5	1	3	0	60%
Poland	19	26	4	14	0	74%
Portugal	11	11	5	6	0	55%
Qatar	1	3	1	0	0	0%
Romania	5	8	3	3	0	60%
Russia	14	18	5	6	0	43%
South Africa	1	1	0	1	0	100%
Spain	56	73	11	39	0	70%
Sweden	31	45	0	28	0	90%
Switzerland	27	44	3	16	0	59%
Turkey	18	22	4	10	0	56%
Ukraine	2	4	1	0	1	50%
United Kingdom	426	505	34	344	2	81%
Europe, Middle East, India, Africa Total	1,544	2,227	201	1,081	8	71%
Latin America						
Argentina	2	2	1	0	0	0%
Brazil	734	4,853	12	70	547	84%
Chile	4	6	1	1	0	25%
Colombia	2	3	1	1	0	50%
Costa Rica	1	1	0	1	0	100%
Ecuador	1	1	0	1	0	100%
Latin America Total	744	4,866	15	74	547	83%
North America						
Canada	22	33	0	20	0	91%
Mexico	1	3	0	1	0	100%
United States of America	4,095	31,780	98	1,921	1,724	89%
North America Total	4,118	31,816	98	1,942	1,724	89%
Worldwide Total	7,480	42,720	373	3,981	2,282	84%

[1] Only countries / regions where Apple received account requests during report period July 1 - December 31, 2019, 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, 2019

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	12	30	12
New Zealand	2	11	1
South Korea	1	1	1
Asia Pacific Total	15	42	14
Europe, Middle East, India, Africa			
Belgium	2	2	0
Denmark	3	8	8
Finland	5	11	8
France	1	1	0
Germany	13	22	18
India	2	4	1
Ireland	5	5	4
Italy	5	7	6
Netherlands	5	6	5
North Macedonia	2	2	2
Norway	2	5	5
Portugal	2	2	2
Spain	1	1	1
Sweden	13	21	19
Switzerland	1	1	0
Ukraine	1	1	1
United Kingdom	48	78	63
Europe, Middle East, India, Africa Total	111	177	143
Latin America			
Argentina	3	3	3
Brazil	98	663	344
Latin America Total	101	666	347
North America			
Canada	16	30	23
Mexico	2	4	3
United States of America	2,522	6,741	4,798
North America Total	2,540	6,775	4,824
Worldwide Total	2,767	7,660	5,328

[1] Only countries / regions where Apple received account preservation requests during report period July 1 - December 31, 2019, 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, 2019

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, except in situations where the case has been verified by Apple to relate to child endangerment.

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 Requests Where Account Restricted	# of Requests Where Account Deleted
Asia Pacific					
Japan	1	1	0	1	0
Asia Pacific Total	1	1	0	1	0
Europe, Middle East, India, Africa					
Denmark	1	1	0	1	0
India	1	1	0	1	0
Sweden	1	1	0	1	0
United Kingdom	2	2	0	1	1
Europe, Middle East, India, Africa Total	5	5	0	4	1
North America					
United States of America	5	5	0	4	1
North America Total	5	5	0	4	1
Worldwide Total	11	11	0	9	2

[1] Only countries / regions where Apple received account restriction/deletion requests during report period July 1 - December 31, 2019, 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 Requests Where Account Restricted	The number of requests where Apple determined the request and order sufficiently demonstrated the account to be restricted was used unlawfully and we proceeded with restriction. We count each request where we proceeded with account restriction and report the total number of such instances by country/region.
# of Requests Where Account Deleted	The number of 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 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, 2019

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	5	0	1	4	80%
China mainland	2	0	0	2	100%
Japan	7	0	0	7	100%
Taiwan	1	0	0	1	100%
Asia Pacific Total	15	0	1	14	93%
Europe, Middle East, India, Africa					
Austria	5	0	0	5	100%
France	9	0	0	9	100%
Germany	22	0	2	20	91%
Greece	2	0	0	2	100%
India	3	0	0	3	100%
Israel	2	0	0	2	100%
Malta	3	0	0	3	100%
Netherlands	11	0	1	10	91%
Norway	2	0	0	2	100%
Poland	1	0	1	0	0%
Qatar	1	0	0	1	100%
Sweden	1	0	1	0	0%
Switzerland	13	0	1	12	92%
Turkey	1	0	0	1	100%
United Kingdom	423	3	35	385	91%
Europe, Middle East, India, Africa Total	499	3	41	455	91%
Latin America					
Brazil	13	0	1	12	92%
Chile	1	0	0	1	100%
Latin America Total	14	0	1	13	93%
North America					
Canada	55	0	3	52	95%
Mexico	3	0	0	3	100%
United States of America	249	3	31	215	86%
North America Total	307	3	34	270	88%
Worldwide Total	835	6	77	752	90%

[1] Only countries / regions where Apple received emergency requests during report period July 1 - December 31, 2019, 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, 2019

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 national security requests received for Apple users/accounts (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	15,500 - 15,999
FISA Content Requests	0 - 499	17,500 - 17,999
National Security Letters	2 - 499	1,505 - 1,999
National Security Letters where non-disclosure order lifted	2	

The below table identifies the two National Security Letters received during this reporting period 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-19-483160	7/23/19	7/15/20
NSL-19-499673	10/17/19	7/24/20

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 for Apple users/accounts and report the total number of orders and National Security Letters received within bands/ranges 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, 2019

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
5,271	496	N/A	1	157	4,617
% of Total (100%)	9%	-	~0%	3%	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
582	92	N/A	0	37	453
% of Total (100%)	16%	-	0%	6%	78%

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
4,095	1,937	0	45	320	1,793
% of Total (100%)	47%	0%	1%	8%	44%

# 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 the offense to 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, 2019

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
202	39	101	62
% of Total (100%)	19%	50%	31%

# 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, 2019

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.

**Table 13: Worldwide Government App Store Takedown Requests - Legal Violations
July 1 - December 31, 2019**

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.

(App removals were limited to requesting country/region App Store storefront)

Country or Region[1]	# of Legal Violation Takedown Requests Received	# of Apps Specified in the Requests	# of Requests Objected to in Part or Rejected in Full	# of Requests Where App Removed	# of Apps Removed	# of Appeals Received	# of Appeals Granted	# of Apps Reinstated
Asia Pacific								
China mainland[2]	47	203	3	45	187	0	0	0
Vietnam[3]	2	33	2	0	0	0	0	0
Asia Pacific Total	49	236	5	45	187	0	0	0
Europe, Middle East, India, Africa								
Austria[4]	1	18	0	1	18	0	0	0
Hungary[5]	1	1	1	0	0	0	0	0
India[5]	1	1	0	1	1	1	1	1
Russia[6]	2	2	1	1	1	0	0	0
Europe, Middle East, India, Africa Total	5	22	2	3	20	1	1	1
Worldwide Total	54	258	7	48	207	1	1	1

[1] Only countries / regions where Apple received legal violation removal requests during report period July 1 - December 31, 2019, are listed.

[2] Requests predominantly related to apps with pornography, illegal content, and apps operating without government license.

[3] Requests related to gaming apps operating without government approval and gambling apps.

[4] Request related to illegal gambling apps.

[5] Request related to app operating without government license.

[6] Requests related to gambling apps.

# 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 Objected to in Part or Rejected in Full

The number of app takedown requests related to alleged/suspected legal violations that resulted in Apple objecting to 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.

# of Appeals Received

The number of App Store takedown requests where Apple received notice of an appeal to court or government agency. We count each app takedown appeal related to alleged/suspected legal violations.

# of Appeals Granted

The number of App Store takedown requests where Apple received notice of a court or government agency granting an appeal to the takedown request. We count each app takedown appeal granted that related to alleged/suspected legal violations.

# of Apps Reinstated

The number of apps reinstated to the App Store due to a court or government agency appeal being granted. We count each app reinstated from app removal related to alleged/suspected legal violations.

Table 14: Worldwide Government App Store Takedown Requests - Platform Policy Violations
July 1 - December 31, 2019

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.

(App removals were worldwide)

Country or Region[1]	# of Platform Policy Violation Takedown Requests Received	# of Apps Specified in the Requests	# of Requests Objected to in Part or Rejected in Full	# of Requests Where App Removed	# of Apps Removed	# of Appeals Received	# of Appeals Granted	# of Apps Reinstated
Asia Pacific								
China mainland[2]	15	35	0	15	35	0	0	0
Asia Pacific Total	15	35	0	15	35	0	0	0
Latin America								
Brazil[3]	1	1	0	1	1	0	0	0
Latin America Total	1	1	0	1	1	0	0	0
North America								
Canada[4]	1	1	0	1	1	0	0	0
North America Total	1	1	0	1	1	0	0	0
Worldwide Total	17	37	0	17	37	0	0	0

[1] Only countries / regions where Apple received platform violation removal requests during report period July 1 - December 31, 2019, are listed.
[2] Requests related to gambling apps violating App Store Review Guidelines.
[3] Request related to education app violating App Store Review Guidelines.
[4] Request related to app facilitating illegal activity in violation of App Store Review Guidelines.

# 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 Objected to in Part or Rejected in Full	The number of app takedown requests related to alleged/suspected platform policy violations that resulted in Apple objecting to 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.
# of Appeals Received	The number of App Store takedown requests where Apple received notice of an appeal to court or government agency. We count each app takedown appeal related to alleged/suspected platform policy violations.
# of Appeals Granted	The number of App Store takedown requests where Apple received notice of a court or government agency granting an appeal to the takedown request. We count each app takedown appeal granted that related to alleged/suspected platform policy violations.
# of Apps Reinstated	The number of apps reinstated to the App Store due to a court or government agency appeal being granted. We count each app reinstated from app removal related to alleged/suspected platform policy violations.

Matters of note in this report:

Government requests related to customer data / accounts

Table 1 Worldwide Government Device Requests

China mainland - High number of devices specified in requests predominantly due to a tax investigation.

Chile - High number of devices specified in requests predominantly due to a cargo theft investigation.

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

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

South Africa - High number of devices specified in requests predominantly due to cargo theft investigations.

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 return and repair fraud investigations.

Table 2 Worldwide Government Financial Identifier Requests

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

Japan - High number of financial identifiers specified in requests predominantly due to an investigation of unauthorized access to iTunes Gift Cards.

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

United Kingdom - High number of financial identifiers specified in requests predominantly due to a tax fraud investigation.

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 court orders where investigation type was not indicated and investigations related to non-violent crime and drug investigations.

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

United States - High number of accounts specified in requests predominantly due to fraud and cyber intrusion investigations and a third party app related investigation.

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 12 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 apps.

China mainland - Requests predominantly related to apps with pornography, illegal content, and apps operating without government license.

Hungary - Request related to app operating without government license.

India - Request related to app operating without government license. Developer appealed. The original Court order was stayed pending appeal and the app was restored.

Russia - Requests related to gambling apps.

Vietnam - Requests related to gaming apps operating without government approval and gambling apps.

Table 14 Worldwide Government App Store Takedown Requests - Platform Policy Violations

Brazil - Request related to education app violating App Store Review Guidelines.

Canada - Request related to app facilitating illegal activity in violation of App Store Review Guidelines.

China mainland - Requests related to gambling apps violating App Store Review Guidelines.