

# Apple Transparency Report: Government and Private Party Requests

## January 1–June 30, 2022

### Introduction

Apple is very seriously committed to protecting your data and we work hard to deliver the most secure hardware, software and services available. We believe our customers have a right to understand how their personal data is managed and protected. This report provides information regarding requests Apple received from government agencies worldwide and U.S. private parties from January 1 through June 30, 2022.

### 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. Apple may also receive requests from government agencies seeking customer data related to specific latitude and longitude coordinates (geofence) for a specified time period. Apple does not have any data to provide in response to geofence requests.

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), Auskunftersuchen (Germany), Obligation de dépôt (Switzerland), 個人情報の開示依頼 (Japan), Personal Data Request (United Kingdom), as well as equivalent court orders and/or requests from other countries.

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 Government Geofence Requests by Legal Process Type
- 12) United States Private Party Requests for Information
- 13) United States Private Party Requests for Account Restriction/Deletion
- 14) Worldwide Government Digital Content Provider Requests

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

## Customer notification

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



**Table 1: Worldwide Government Device Requests  
January 1–June 30, 2022**

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 <sup>1</sup>	# of Device Requests Received	# of Devices Specified in the Requests	# of Device Requests Where Data Provided	% of Device Requests Where Data Provided
<b>Asia Pacific</b>				
Australia	486	811	266	55%
China mainland	1,481	167,854	1,407	95%
Hong Kong	27	49	4	15%
Japan	397	861	342	86%
Macau	1	3	1	100%
Mongolia	1	1	0	0%
New Zealand	16	20	1	6%
Philippines	1	25	0	0%
Singapore	771	816	660	86%
South Korea	43	298	26	60%
Taiwan	94	160	41	44%
Thailand	3	3	1	33%
<b>Asia Pacific Total</b>	<b>3,321</b>	<b>170,901</b>	<b>2,749</b>	<b>83%</b>
<b>Europe, Middle East, India, Africa</b>				
Andorra	24	25	21	88%
Austria	52	141	3	6%
Belgium	72	157	40	56%
Bosnia and Herzegovina	1	3	0	0%
Bulgaria	1	1	0	0%
Czech Republic	76	840	53	70%
Denmark	8	23	5	63%
Estonia	1	2	0	0%
Finland	2	4	2	100%
France	686	3,164	370	54%
Germany	11,999	17,623	8,806	73%
Greece	8	40	0	0%
Hungary	19	157	11	58%
India	98	145	13	13%
Ireland	61	544	36	59%
Israel	7	17	4	57%
Italy	174	353	30	17%
Lithuania	2	3	1	50%
Luxembourg	4	7	2	50%
Moldova	1	1	0	0%
Netherlands	39	580	22	56%
Norway	10	17	0	0%
Poland	28	80	4	14%
Portugal	60	122	14	23%
Romania	11	19	6	55%
Russia	128	215	14	11%
Slovenia	14	18	10	71%
South Africa	4	64	3	75%
Spain	1,206	2,512	884	73%
Sweden	156	404	130	83%
Switzerland	100	499	46	46%
Türkiye	24	24	8	33%
Ukraine	2	2	1	50%
United Arab Emirates	1	2	0	0%
United Kingdom	882	1,369	683	77%
<b>Europe, Middle East, India, Africa Total</b>	<b>15,961</b>	<b>29,177</b>	<b>11,222</b>	<b>70%</b>
<b>Latin America</b>				
Argentina	6	9	1	17%
Brazil	3,759	15,370	3,375	90%
Chile	313	572	256	82%
Colombia	2	2	0	0%
<b>Latin America Total</b>	<b>4,080</b>	<b>15,953</b>	<b>3,632</b>	<b>89%</b>

<sup>1</sup> Only countries / regions where Apple received device requests during report period January 1–June 30, 2022 are listed.



**Table 1: Worldwide Government Device Requests (continued)  
January 1–June 30, 2022**

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 <sup>1</sup>	# of Device Requests Received	# of Devices Specified in the Requests	# of Device Requests Where Data Provided	% of Device Requests Where Data Provided
North America				
Canada	46	75	42	91%
Mexico	3	3	1	33%
United States of America	5,611	19,253	4,582	82%
North America Total	5,660	19,331	4,625	82%
Worldwide Total	29,022	235,362	22,228	77%

<sup>1</sup> Only countries / regions where Apple received device requests during report period January 1–June 30, 2022 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 January 1–June 30, 2022

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 <sup>1</sup>	# 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
<b>Asia Pacific</b>				
Australia	48	144	14	29%
China mainland	55	1,792	46	84%
Hong Kong	241	1,375	175	73%
Japan	189	864	144	76%
Macau	13	69	12	92%
Singapore	316	2,931	258	82%
South Korea	116	939	104	90%
Taiwan	782	6,349	355	45%
Thailand	11	11	3	27%
<b>Asia Pacific Total</b>	<b>1,771</b>	<b>14,474</b>	<b>1,111</b>	<b>63%</b>
<b>Europe, Middle East, India, Africa</b>				
Austria	31	108	3	10%
Belgium	6	12	3	50%
Bulgaria	3	5	1	33%
Croatia	1	1	1	100%
Czech Republic	25	246	10	40%
Denmark	3	3	2	67%
Estonia	1	1	0	0%
Finland	3	22	2	67%
France	331	607	179	54%
Germany	876	2,437	528	60%
Greece	9	59	0	0%
Hungary	30	30	9	30%
India	83	83	4	5%
Ireland	34	327	16	47%
Italy	149	355	7	5%
Kosovo	1	1	0	0%
Latvia	1	1	0	0%
Lithuania	4	4	0	0%
Netherlands	2	4	2	100%
Norway	2	26	0	0%
Pakistan	3	3	0	0%
Poland	35	83	0	0%
Portugal	47	106	19	40%
Romania	82	86	48	59%
Russia	41	41	3	7%
Slovakia	2	2	0	0%
Spain	890	1,306	450	51%
Sweden	11	12	7	64%
Switzerland	60	669	30	50%
Türkiye	410	419	230	56%
Ukraine	2	2	0	0%
United Arab Emirates	1	17	0	0%
United Kingdom	27	49	3	11%
<b>Europe, Middle East, India, Africa Total</b>	<b>3,206</b>	<b>7,127</b>	<b>1,557</b>	<b>49%</b>
<b>Latin America</b>				
Brazil	2	2	1	50%
Chile	1	1	1	100%
Costa Rica	1	1	1	100%
Paraguay	1	2	0	0%
Peru	2	2	0	0%
<b>Latin America Total</b>	<b>7</b>	<b>8</b>	<b>3</b>	<b>43%</b>
<b>North America</b>				
Canada	11	24	9	82%
United States of America	985	3,707	734	75%
<b>North America Total</b>	<b>996</b>	<b>3,731</b>	<b>743</b>	<b>75%</b>
<b>Worldwide Total</b>	<b>5,980</b>	<b>25,340</b>	<b>3,414</b>	<b>57%</b>

<sup>1</sup> Only countries / regions where Apple received financial identifier requests during report period January 1–June 30, 2022 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  
January 1–June 30, 2022**

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 <sup>1</sup>	# 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
<b>Asia Pacific</b>						
Australia	161	224	26	102	1	64%
Bangladesh	1	1	1	0	0	0%
China mainland	43	289	2	23	10	77%
Hong Kong	4	7	1	2	0	50%
Japan	412	586	16	312	0	76%
Macau	2	2	0	2	0	100%
Singapore	46	53	4	26	0	57%
South Korea	44	50	0	35	0	80%
Taiwan	312	676	142	157	0	50%
Thailand	1	1	1	0	0	0%
<b>Asia Pacific Total</b>	<b>1,026</b>	<b>1,889</b>	<b>193</b>	<b>659</b>	<b>11</b>	<b>65%</b>
<b>Europe, Middle East, India, Africa</b>						
Andorra	5	5	0	3	0	60%
Austria	17	18	14	3	0	18%
Belgium	42	55	2	35	0	83%
Czech Republic	20	25	1	12	0	60%
Denmark	4	4	0	3	1	100%
Estonia	1	1	1	0	0	0%
Finland	5	6	0	4	0	80%
France	392	541	42	256	0	65%
Germany	860	1,306	100	613	0	71%
Greece	7	7	7	0	0	0%
Hungary	3	3	1	0	0	0%
India	36	47	24	3	0	8%
Ireland	33	42	9	24	0	73%
Israel	9	35	1	5	0	56%
Italy	114	136	31	50	0	44%
Kosovo	1	1	1	0	0	0%
Luxembourg	2	13	0	2	0	100%
Malta	4	4	2	2	0	50%
Moldova	1	1	1	0	0	0%
Monaco	1	1	1	0	0	0%
Netherlands	48	145	7	34	0	71%
Norway	5	7	4	0	0	0%
Poland	34	61	22	7	0	21%
Portugal	7	8	1	5	0	71%
Qatar	1	4	0	1	0	100%
Romania	6	8	1	4	0	67%
Russia	24	32	20	1	0	4%
Slovakia	1	1	1	0	0	0%
Spain	79	114	23	34	0	43%
Sweden	72	119	1	64	1	90%
Switzerland	27	37	8	17	1	67%
Türkiye	25	28	12	9	0	36%
Ukraine	2	3	0	1	1	100%
United Kingdom	950	1,134	13	828	0	87%
<b>Europe, Middle East, India, Africa Total</b>	<b>2,838</b>	<b>3,952</b>	<b>351</b>	<b>2,020</b>	<b>4</b>	<b>71%</b>
<b>Latin America</b>						
Argentina	5	6	3	1	0	20%
Bermuda	1	2	0	0	1	100%
Brazil	2,135	13,392	7	476	1,289	83%
Chile	9	9	0	4	1	56%
Colombia	1	2	1	0	0	0%
Costa Rica	1	1	1	0	0	0%
Paraguay	2	2	2	0	0	0%
<b>Latin America Total</b>	<b>2,154</b>	<b>13,414</b>	<b>14</b>	<b>481</b>	<b>1,291</b>	<b>82%</b>
<b>North America</b>						
Canada	37	45	1	29	0	78%
Mexico	6	7	1	3	0	50%
United States of America	7,944	52,749	507	3,795	3,354	90%
<b>North America Total</b>	<b>7,987</b>	<b>52,801</b>	<b>509</b>	<b>3,827</b>	<b>3,354</b>	<b>90%</b>
<b>Worldwide Total</b>	<b>14,005</b>	<b>72,056</b>	<b>1,067</b>	<b>6,987</b>	<b>4,660</b>	<b>83%</b>

<sup>1</sup> Only countries / regions where Apple received account requests during report period January 1–June 30, 2022 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  
January 1–June 30, 2022**

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 <sup>1</sup>	# of Account Preservation Requests Received	# of Accounts Specified in the Requests	# of Accounts Where Data Preserved
<b>Asia Pacific</b>			
Australia	15	28	22
Indonesia	2	4	4
Japan	1	1	1
New Zealand	2	3	2
<b>Asia Pacific Total</b>	<b>20</b>	<b>36</b>	<b>29</b>
<b>Europe, Middle East, India, Africa</b>			
Austria	9	24	19
Belgium	7	9	7
Denmark	12	23	12
Finland	3	6	5
France	9	26	24
Germany	53	82	75
Greece	1	2	2
India	2	7	6
Ireland	29	34	33
Italy	2	2	2
Luxembourg	1	1	1
Netherlands	12	27	18
North Macedonia	1	1	1
Norway	4	18	5
Poland	4	13	13
Russia	1	1	1
Slovenia	1	1	1
South Africa	3	7	3
Spain	2	2	2
Sweden	11	21	19
Switzerland	12	18	18
Türkiye	5	7	7
Ukraine	1	1	1
United Kingdom	57	97	89
<b>Europe, Middle East, India, Africa Total</b>	<b>242</b>	<b>430</b>	<b>364</b>
<b>Latin America</b>			
Argentina	3	3	3
Brazil	187	1179	787
Chile	1	1	1
Peru	1	1	1
<b>Latin America Total</b>	<b>192</b>	<b>1,184</b>	<b>792</b>
<b>North America</b>			
Canada	32	65	48
Mexico	3	5	3
United States of America	4,799	14,829	11,126
<b>North America Total</b>	<b>4,834</b>	<b>14,899</b>	<b>11,177</b>
<b>Worldwide Total</b>	<b>5,288</b>	<b>16,549</b>	<b>12,362</b>

<sup>1</sup> Only countries / regions where Apple received account preservation requests during report period January 1–June 30, 2022 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  
January 1–June 30, 2022**

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 <sup>1</sup>	# 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
<b>Asia Pacific</b>					
Australia	2	3	0	2	0
Japan	1	1	0	1	0
Asia Pacific Total	3	4	0	3	0
<b>Europe, Middle East, India, Africa</b>					
Belgium	1	4	1	0	0
Finland	1	2	0	1	0
Norway	3	6	0	3	0
United Kingdom <sup>2</sup>	15	16	0	14	0
Europe, Middle East, India, Africa Total	20	28	1	18	0
<b>Latin America</b>					
Brazil	1	1	1	0	0
Latin America Total	1	1	1	0	0
<b>North America</b>					
Canada	2	2	0	2	0
United States of America	11	11	2	9	0
North America Total	13	13	2	11	0
Worldwide Total	37	46	4	32	0

<sup>1</sup> Only countries / regions where Apple received account restriction/deletion requests during report period January 1–June 30, 2022 are listed.

<sup>2</sup> One request received where Apple had no results for the account identified in the request.

**# 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  
January 1–June 30, 2022**

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 <sup>1</sup>	# 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
<b>Asia Pacific</b>					
Australia	14	0	3	11	79%
Japan	112	1	8	103	92%
New Zealand	2	0	0	2	100%
Singapore	6	0	0	6	100%
Taiwan	1	0	0	1	100%
<b>Asia Pacific Total</b>	<b>135</b>	<b>1</b>	<b>11</b>	<b>123</b>	<b>91%</b>
<b>Europe, Middle East, India, Africa</b>					
Austria	3	0	0	3	100%
Belgium	2	0	1	1	50%
Czech Republic	1	0	0	1	100%
Denmark	2	0	1	1	50%
France	19	1	1	17	89%
Germany	33	2	0	31	94%
India	10	3	3	4	40%
Ireland	1	0	0	1	100%
Israel	2	0	1	1	50%
Italy	5	2	0	3	60%
Netherlands	8	0	1	7	88%
Norway	4	0	0	4	100%
Oman	1	0	1	0	0%
Poland	4	0	0	4	100%
Slovenia	1	0	0	1	100%
South Africa	4	0	1	3	75%
Spain	3	0	2	1	33%
Sweden	6	0	1	5	83%
Switzerland	19	0	0	19	100%
Türkiye	1	0	0	1	100%
Ukraine	1	0	0	1	100%
United Kingdom	589	3	40	546	93%
<b>Europe, Middle East, India, Africa Total</b>	<b>719</b>	<b>11</b>	<b>53</b>	<b>655</b>	<b>91%</b>
<b>Latin America</b>					
Brazil	59	1	3	55	93%
Chile	1	0	1	0	0%
Colombia	1	0	0	1	100%
<b>Latin America Total</b>	<b>61</b>	<b>1</b>	<b>4</b>	<b>56</b>	<b>92%</b>
<b>North America</b>					
Canada	76	1	10	65	86%
Mexico	1	0	0	1	100%
United States of America	432	6	50	376	87%
<b>North America Total</b>	<b>509</b>	<b>7</b>	<b>60</b>	<b>442</b>	<b>87%</b>
<b>Worldwide Total</b>	<b>1,424</b>	<b>20</b>	<b>128</b>	<b>1,276</b>	<b>90%</b>

<sup>1</sup> Only countries / regions where Apple received emergency requests during report period January 1–June 30, 2022 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, or in certain instances customers' iCloud content, such as stored photos, email, iOS device backups, contacts or calendars, in response to a valid emergency request. We count each emergency request where we provide data and report the total number of such instances by country/region.

**% of Emergency Requests Where Data Provided**

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



## Table 7: United States Government National Security Requests January 1–June 30, 2022

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. Apple responds to National Security FISA content requests with information obtained from iCloud. Under the law, Apple cannot further disclose what information or data may be sought through these requests.

National Security Request Type	# of Requests Received	# of Users/Accounts
FISA Non-Content Requests	0–499	38,000–38,499
FISA Content Requests	0–499	33,500–33,999
National Security Letters	2–499	503–999
National Security Letters where non-disclosure order lifted	2	

The below table identifies the 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-22-545095	3/21/22	11/7/22
NSL-22-545835	4/15/22	11/9/22

### 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.



## Tables 8, 9, 10, 11: United States Government Requests by Legal Process Type January 1–June 30, 2022

Tables 8, 9, 10, and 11 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
5,611	897	N/A	2	140	4,572
% of Total (100%)	16%	-	~0%	2.5%	81.5%

### 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
985	171	N/A	0	42	772
% of Total (100%)	17.3%	-	-	4.3%	78.4%

### 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
7,944	3,697	1	85	558	3,603
% of Total (100%)	47%	~0%	1%	7%	45%

### Table 11: United States Government Geofence Requests by Legal Process Type

Table 11 provides information regarding search warrants Apple received as Geofence Requests. Apple does not have any data to provide in response to geofence warrants.

# of Geofence Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
13	13	N/A	N/A	N/A	N/A
% of Total (100%)	100%	-	-	-	-



### **# 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.

### **# of Geofence Requests**

The total number of United States government requests Apple received seeking customer data related to specific latitude and longitude coordinates (geofence) for a specified time period. We count each individual request received from government agencies and report the total number of requests received. Apple does not have any data to provide in response to Geofence Requests.

### **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 12: United States Private Party Requests for Information  
January 1–June 30, 2022**

Table 12 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
254	218	17	19
% of Total (100%)	85.8%	6.7%	7.5%

**# 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 13: United States Private Party Requests for Account Restriction/Deletion  
January 1–June 30, 2022**

Table 13 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 14: Worldwide Government Digital Content Provider Requests  
January 1–June 30, 2022**

Table 14 provides information regarding government requests received where digital content provider information is requested. Examples of such requests are where law enforcement agencies are investigating a digital content provider who may have provided a service or content (e.g. app, music, or podcast) that is alleged/suspected to violate local law. These requests generally seek details of the content provider, such as name, email address, physical address, and in certain instances payment details or other information.

Country or Region <sup>1</sup>	# of Content Provider Requests Received	# of Content Provider Requests Objected to in Part or Rejected in Full	# of Content Provider Requests Where Data Provided	% of Content Provider Requests Where Data Provided
<b>Asia Pacific</b>				
China mainland	10	2	4	40%
Hong Kong	2	1	1	50%
Japan	1	0	1	100%
Singapore	2	1	0	0%
Taiwan	1	0	1	100%
<b>Asia Pacific Total</b>	<b>16</b>	<b>4</b>	<b>7</b>	<b>44%</b>
<b>Europe, Middle East, India, Africa</b>				
Austria	1	0	1	100%
France	2	0	1	50%
Germany	3	0	3	100%
Hungary	1	1	0	0%
India	1	1	0	0%
Poland	2	1	1	50%
Türkiye	1	1	0	0%
<b>Europe, Middle East, India, Africa Total</b>	<b>11</b>	<b>4</b>	<b>6</b>	<b>55%</b>
<b>Latin America</b>				
Brazil	1	0	1	100%
<b>Latin America Total</b>	<b>1</b>	<b>0</b>	<b>1</b>	<b>100%</b>
<b>North America</b>				
United States of America	12	0	12	100%
<b>North America Total</b>	<b>12</b>	<b>0</b>	<b>12</b>	<b>100%</b>
<b>Worldwide Total</b>	<b>40</b>	<b>8</b>	<b>26</b>	<b>65%</b>

<sup>1</sup> Only countries / regions where Apple received digital content provider requests during report period January 1–June 30, 2022 are listed.

**# of Content Provider Requests Received**

The number of requests received from government agencies seeking digital content provider information related to specific digital content identifiers, such as digital asset ID, content provider ID, or digital content name. 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 Content Provider Requests Objected to in Part or Rejected in Full**

The number of digital content provider-based requests that resulted in Apple objecting to or rejecting the request in part or in full based on grounds such as a request that 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 to be excessively broad for the case in question. We count each digital content provider-based request where we object in part or reject in full and report the total number of such instances by country/region.

**# of Content Provider Requests Where Data Provided**

The number of digital content provider requests that resulted in Apple providing data, such as content provider name and contact information associated with a specific app, music item, or podcast, in response to a valid legal request. We count each digital content provider request where we provide data and report the total number of such instances by country/region.

**% of Content Provider Requests Where Data Provided**

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



## **Worldwide Government App Store Takedown Requests January 1–December 31, 2022**

Beginning with the 2022 calendar year, Apple publishes government App Store takedown requests in a dedicated [App Store Transparency Report](#) that includes data showing takedown demands by government entity and law cited. See <https://www.apple.com/legal/more-resources/>.



**Matters of note in this report:**

**Government requests related to customer data / accounts**

**Table 1 Worldwide Government Device Requests**

Brazil - High volume of device requests predominantly due to investigations related to non-violent crime, drugs, and stolen devices. High number of devices specified in requests predominantly due to non-violent crime and drug investigations.

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

Germany - High volume of device requests and high number of devices specified in requests predominantly due to stolen device investigations.

United States of America - High volume of device requests predominantly due to stolen device investigations and requests where investigation type was not indicated. High number of devices specified in requests predominantly due to a counterfeit product investigation, stolen device investigations and requests where investigation type was not indicated.

**Table 2 Worldwide Government Financial Identifier Requests**

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

Taiwan - High number of financial identifiers specified in requests predominantly due to financial fraud investigations involving Apple Media Services purchases and Apple Gift Cards.

**Table 3 Worldwide Government Account Requests**

Brazil - High volume of account requests and 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 drugs.

United States of America - High volume of account requests predominantly due to legal requests where investigation type was not indicated. High number of account identifiers specified in requests were due to a single large criminal investigation involving only non-content data.

**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 identified 20 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.