Apple Transparency Report: Government and Private Party Requests

January 1–June 30, 2024

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, 2024.

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.

Digital Content Provider government request circumstances generally relate to law enforcement investigations where a service or content (such as an app, music item, or podcast) is suspected to violate local law.

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, account restriction/deletion, emergency, digital content provider, and United States private party requests, and report these numbers accordingly.

We count the number of discernible devices, financial identifiers, accounts and/or push tokens 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 Push Token Requests
7) Worldwide Government Emergency Requests
8) US-UK Data Access Agreement: Warrant Requests from the UK
9) United States Government National Security Requests
10) United States Government Device Requests by Legal Process Type
11) United States Government Financial Identifier Requests by Legal Process Type
12) United States Government Account Requests by Legal Process Type
13) United States Government Push Token Requests by Legal Process Type
14) United States Government Geofence Requests by Legal Process Type
15) United States Private Party Requests for Information
16) United States Private Party Requests for Account Restriction/Deletion
17) 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. For United States-United Kingdom Data Access Agreement (CLOUD) Investigatory Powers Act warrant requests, Apple is required by law to delay reporting by 6 months and report the numbers in ranges of 500, pursuant to 2018 No. 349.

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, 2024

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	721	962	212	29%
China mainland	1,212	365,980	1,146	95%
Hong Kong	172	533	1	1%
Japan	753	2,690	517	69%
Macau	1	36	1	100%
Malaysia	5	41	4	80%
New Zealand	68	74	2	3%
Singapore	489	528	340	70%
South Korea	50	88	25	50%
Taiwan	29	70	15	52%
Thailand	23	27	3	13%
Vietnam	2	2	0	0%
Asia Pacific Total	3,525	371,031	2,266	64%
Europe, Middle East, India, Africa				
Albania	1	3	0	0%
Austria	48	85	15	31%
Belarus	3	5	0	0%
Belgium	92	192	58	63%
Bosnia and Herzegovina	1	8	0	0%
Croatia	1	11	0	0%
Czech Republic	101	324	60	59%
Denmark	19	21	5	26%
Estonia	2	2	0	0%
Finland	10	16	3	30%
France	970	1,946	439	45%
Germany	9,778	80,848	4,713	48%
Greece	18	26	0	0%
Hungary	16	44	7	44%
India	203	656	48	24%
Ireland	99	2,725	45	45%
Israel	19	23	13	68%
Italy	255	887	29	11%
Lithuania	1	1	1	100%
Luxembourg	7	15	4	57%
Malta	3	4	1	33%
Monaco	1	1	0	0%
Netherlands	126	286	59	47%
Norway	27	49	24	89%
Poland	75	252	17	23%
Portugal	376	450	4	1%
Romania	11	52	3	27%
Russia	13	17	1	8%
Serbia	1	2	0	0%
Slovakia	2	2	1	50%
Slovenia	3	8	3	100%
South Africa	9	12	5	56%
Spain	540	1,446	186	34%
Sweden	125	379	92	74%
Switzerland	82	298	49	60%
Türkiye	33	34	5	15%
Ukraine	5	13	0	0%
United Arab Emirates	2	2	0	0%
United Kingdom	2,925	8,211	2,278	78%
Europe, Middle East, India, Africa Total	16,003	99,356	8,168	51%
Latin America				
Argentina	6	9	1	17%
Brazil	8,776	42,276	6,808	78%
Chile	61	81	31	51%
Colombia	47	94	31	66%
Costa Rica	1	2	0	0%
Ecuador	1	1	0	0%
Jamaica	1	1	0	0%
Latin America Total	8,893	42,464	6,871	77%

Table 1: Worldwide Government Device Requests (continued)
January 1–June 30, 2024

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
North America				
Canada	430	790	239	56%
Mexico	11	22	7	64%
United States of America	12,043	42,747	10,377	86%
North America Total	12,484	43,559	10,623	85%
Worldwide Total	40,905	556,410	27,928	68%

[1] Only countries / regions where Apple received device requests during report period January 1–June 30, 2024 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, 2024

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	122	1,285	37	30%
China mainland	465	3,913	361	78%
Hong Kong	220	702	110	50%
Japan	1,345	11,941	1,142	85%
Macau	24	232	9	38%
New Zealand	1	10	1	100%
Singapore	83	432	57	69%
South Korea	199	1,722	111	56%
Taiwan	4,968	66,041	4,819	97%
Thailand	7	11	1	14%
Asia Pacific Total	7,434	86,289	6,648	89%
Europe, Middle East, India, Africa				
Andorra	4	56	4	100%
Austria	116	1,121	3	3%
Belarus	3	3	1	33%
Belgium	15	208	5	33%
Bulgaria	2	3	0	0%
Czech Republic	28	139	15	54%
Denmark	6	6	2	33%
Finland	19	373	17	89%
France	283	1,068	142	50%
Germany	1,198	5,041	214	18%
Greece	3	3	0	0%
Hungary	93	145	25	27%
India	169	2,570	15	9%
Ireland	40	649	25	63%
Israel	2	2	0	0%
Italy	234	1,062	26	11%
Jordan	1	1	0	0%
Lithuania	4	4	4	100%
Luxembourg	1	1	0	0%
Malta	1	2	1	100%
Nepal	1	1	0	0%
Netherlands	8	74	5	63%
Norway	3	41	1	33%
Poland	60	210	7	12%
Portugal	39	178	16	41%
Romania	16	18	12	75%
San Marino	1	1	0	0%
South Africa	1	1	0	0%
Spain	640	1,473	224	35%
Sweden	30	113	16	53%
Switzerland	98	974	59	60%
Türkiye	369	387	137	37%
Ukraine	9	11	2	22%
United Arab Emirates	20	25	0	0%
United Kingdom	138	456	9	7%
Europe, Middle East, India, Africa Total	3,655	16,420	987	27%
Latin America				
Argentina	1	6	0	0%
Brazil	12	68	2	17%
Chile	1	3	0	0%
Costa Rica	7	7	2	29%
Peru	2	2	0	0%
Latin America Total	23	86	4	17%

Table 2: Worldwide Government Financial Identifier Requests (continued) January 1–June 30, 2024

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
North America				
Canada	79	446	59	75%
Mexico	1	1	0	0%
United States of America	1,341	6,366	930	69%
North America Total	1,421	6,813	989	70%
Worldwide Total	12,533	109,608	8,628	69%

[1] Only countries / regions where Apple received financial identifier requests during report period January 1–June 30, 2024 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, 2024

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	303	620	41	172	0	57%
China mainland	398	1768	8	256	67	81%
Hong Kong	5	35	1	4	0	80%
Japan	841	1235	65	650	0	77%
Macau	4	19	2	2	0	50%
New Zealand	9	16	2	6	0	67%
Singapore	32	41	7	17	0	53%
South Korea	57	119	0	38	0	67%
Taiwan	185	345	8	139	0	75%
Vietnam	2	2	2	0	0	0%
Asia Pacific Total	1,836	4,200	136	1,284	67	74%
Europe, Middle East, India, Africa						
Austria	74	82	28	30	4	46%
Azerbaijan	2	2	0	2	0	100%
Belarus	4	6	3	1	0	25%
Belgium	76	98	8	68	0	89%
Bulgaria	3	4	1	0	0	0%
Croatia	5	8	1	2	0	40%
Cyprus	1	1	0	1	0	100%
Czech Republic	170	215	5	128	5	78%
Denmark	4	9	0	4	0	100%
Estonia	2	2	1	0	0	0%
Finland	18	40	1	10	7	94%
France	8	8	0	0	8	100%
Germany	2,655	3,425	353	1,718	12	65%
Greece	5	8	2	0	0	0%
Hungary	44	50	21	13	0	30%
India	154	669	75	25	0	16%
Ireland	72	119	5	48	3	71%
Israel	15	20	1	10	0	67%
Italy	123	231	31	40	0	33%
Kyrgyzstan	1	1	0	0	0	0%
Libya	3	5	0	1	0	33%
Lithuania	3	3	2	1	0	33%
Luxembourg	3	3	0	3	0	100%
Malawi	1	1	1	0	0	0%
Malta	4	4	0	3	0	75%
Moldova	1	3	0	0	0	0%
Nepal	5	6	2	0	0	0%
Netherlands	110	260	15	55	0	50%
North Macedonia	2	2	2	0	0	0%
Norway	29	59	2	19	0	66%
Poland	201	246	114	39	3	21%
Portugal	23	47	11	6	3	39%
Romania	4	6	2	2	0	50%
Russia	3	3	3	0	0	0%
Slovakia	3	3	0	2	0	67%
Slovenia	5	6	5	0	0	0%
South Africa	3	3	1	2	0	67%
Spain	156	240	38	56	0	36%
Sweden	192	303	5	157	0	82%
Switzerland	103	182	22	40	20	58%
Türkiye	29	32	15	8	0	28%
United Kingdom	2,550	2,920	31	2,090	2	82%
Europe, Middle East, India, Africa Total	6,869	9,335	807	4,584	67	68%

Table 3: Worldwide Government Account Requests (continued)
January 1 - June 30, 2024

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
Latin America						
Argentina	11	30	3	1	0	9%
Brazil	3,664	17,884	546	838	1,781	71%
Chile	11	22	3	7	0	64%
Colombia	10	26	5	5	0	50%
Costa Rica	3	3	0	2	0	67%
Dominican Republic	2	29	1	0	0	0%
Ecuador	3	6	1	0	0	0%
Uruguay	1	1	0	1	0	100%
Latin America Total	3,705	18,001	559	854	1,781	71%
North America						
Canada	264	688	11	212	15	86%
Mexico	10	15	3	4	0	40%
United States of America	12,812	40,015	1,427	5,652	5,915	90%
North America Total	13,086	40,718	1,441	5,868	5,930	90%
Worldwide Total	25,496	72,254	2,943	12,590	7,845	80%

[1] Only countries / regions where Apple received account requests during report period January 1–June 30, 2024 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, 2024

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	13	35	26
New Zealand	5	13	7
Singapore	2	2	2
Asia Pacific Total	20	50	35
Europe, Middle East, India, Africa			
Austria	3	4	4
Azerbaijan	1	1	1
Belgium	7	9	8
Bosnia and Herzegovina	2	10	9
Bulgaria	2	3	2
Croatia	1	1	0
Czech Republic	1	3	2
Denmark	13	21	16
Finland	5	9	7
France	41	94	85
Germany	52	60	50
Greece	1	2	1
Hungary	1	2	1
Iceland	1	1	1
India	4	20	9
Ireland	25	42	41
Italy	1	2	2
Latvia	1	1	1
Netherlands	10	14	12
Poland	3	3	1
Portugal	1	1	1
Qatar	1	1	0
Romania	1	2	2
Slovenia	1	1	1
South Africa	1	1	0
Sweden	12	24	23
Switzerland	3	5	5
Ukraine	3	27	25
United Kingdom	64	128	99
Europe, Middle East, India, Africa Total	262	492	409
Latin America			
Bermuda	3	38	37
Brazil	264	762	407
Latin America Total	267	800	444
North America			
Canada	77	84	61
Mexico	1	1	1
United States of America	8,170	26,037	20,513
North America Total	8,248	26,122	20,575
Worldwide Total	8,797	27,464	21,463

[1] Only countries / regions where Apple received account preservation requests during report period January 1–June 30, 2024 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, 2024

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					
Australia	1	1	0	0	1
Singapore	1	1	0	1	0
Asia Pacific Total	2	2	0	1	1
Europe, Middle East, India, Africa					
Germany	5	5	1	2	2
India	1	1	0	1	0
Netherlands	1	1	0	1	0
Europe, Middle East, India, Africa Total	7	7	1	4	2
Latin America					
-	-	-	-	-	-
Latin America Total	0	0	0	0	0
North America					
Canada	1	2	0	2	0
United States of America	40	57	0	35	2
North America Total	41	59	0	37	2
Worldwide Total	50	68	1	42	5

[1] Only countries / regions where Apple received account restriction/deletion requests during report period January 1–June 30, 2024 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 Push Token Requests January 1–June 30, 2024

When users allow a currently installed application to receive notifications, an Apple Push Notification service token (push token) is generated and registered to that developer and device. Table 6 provides information regarding push token-based requests received. Examples of such requests are where law enforcement agencies are working on cases where they suspect the associated Apple Account may have been used unlawfully. Push token-based requests generally seek identifying details of the Apple Account associated with the device's push token, such as name, physical address and email address.

Country or Region[1]	# of Push Token Requests Received	# of Push Tokens Specified in the Requests	# of Push Token Requests Where Data Provided	% of Push Token Requests Where Data Provided
Asia Pacific				
Singapore	1	1	0	0%
Asia Pacific Total	1	1	0	0%
Europe, Middle East, India, Africa				
Germany	4	4	1	25%
Poland	1	2	0	0%
United Kingdom	141	143	127	90%
Europe, Middle East, India, Africa Total	146	149	128	88%
Latin America				
-	-	-	-	-
Latin America Total	0	0	0	-
North America				
Canada	1	25	0	0%
United States of America	129	370	36	28%
North America Total	130	395	36	28%
Worldwide Total	277	545	164	59%

[1] Only countries / regions where Apple received push token requests during report period January 1–June 30, 2024 are listed.

# of Push Token Requests Received

The number of requests received from a government agency seeking customer data related to specific Apple Push Notification service token identifiers (push token). We count each individual request received from each country/region and report the total number of requests received by country/region.

# of Push Tokens Specified in the Requests

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

# of Push Token Requests Where Data Provided

The number of push token-based requests that resulted in Apple providing data. We count each push token-based request where we provide data and report the total number of such instances by country/region.

% of Push Token Requests Where Data Provided

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

Table 7: Worldwide Government Emergency Requests
January 1–June 30, 2024

Table 7 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	26	3	4	19	73%
China mainland	1	1	0	0	0%
Japan	288	26	19	239	83%
New Zealand	3	1	0	2	67%
South Korea	6	2	2	2	33%
Taiwan	3	1	1	1	33%
Asia Pacific Total	327	34	26	263	80%
Europe, Middle East, India, Africa					
Austria	9	2	1	6	67%
Belgium	6	2	0	4	67%
Croatia	1	0	1	0	0%
Cyprus	1	0	0	1	100%
Czech Republic	2	1	0	1	50%
Denmark	1	0	0	1	100%
Finland	2	0	0	2	100%
France	70	13	9	48	69%
Germany	99	15	10	74	75%
Greece	2	1	0	1	50%
Hungary	1	1	0	0	0%
India	60	14	2	44	73%
Ireland	7	2	2	3	43%
Israel	9	0	2	7	78%
Italy	17	2	1	14	82%
Libya	3	0	2	1	33%
Luxembourg	1	0	0	1	100%
Mauritius	1	1	0	0	0%
Netherlands	17	6	0	11	65%
Norway	22	1	3	18	82%
Poland	14	1	2	11	79%
Portugal	2	2	0	0	0%
Romania	2	0	1	1	50%
South Africa	4	2	0	2	50%
Spain	1	0	0	1	100%
Sweden	25	3	5	17	68%
Switzerland	25	3	1	21	84%
United Kingdom	726	20	58	658	91%
Europe, Middle East, India, Africa Total	1,130	92	100	948	84%
Latin America					
Argentina	1	1	0	0	0%
Bolivia	1	1	0	0	0%
Brazil	67	8	4	55	82%
Costa Rica	1	0	0	1	100%
Dominican Republic	1	0	0	1	100%
Latin America Total	71	10	4	57	80%
North America					
Canada	169	12	12	141	83%
Mexico	13	2	2	9	69%
United States of America	793	96	78	601	76%
North America Total	975	110	92	751	77%
Worldwide Total	2,503	246	222	2,019	81%

[1] Only countries / regions where Apple received emergency requests during report period January 1–June 30, 2024 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 8: US-UK Data Access Agreement: Warrant Requests from the UK January 1–June 30, 2024

Table 8 provides information regarding Investigatory Powers Act ("IPA") warrant requests Apple received from the United Kingdom pursuant to the US-UK Data Access Agreement (entered into force on October 3, 2022).

We report these requests received for Apple Accounts within ranges permissible by law pursuant to The Investigatory Powers (Disclosure of Statistical Information) Regulations 2018 ("IP DSI 2018"). Apple is required by law to delay initial reporting for a period of 18 months and report in bands of 500. Apple is required for subsequent reporting periods 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 IP DSI 2018 for reporting this level of detail regarding IPA warrant requests received under the US-UK Data Access Agreement. Under the law, Apple is limited in its ability to disclose what information or data may be sought through these requests.

Request Type	# of Requests Received	# of Users/Accounts
IPA Non-Content Requests	0–499	0–499
IPA Content Requests	500-999	500-999

Request Type

IPA warrant requests issued pursuant to the US-UK Data Access Agreement for content and non-content data. Non-content data is data such as subscriber or transactional information and connection logs. Content data is iCloud data such as stored photos, email, iOS device backups, contacts or calendars.

# of Requests Received

The number of IPA warrant requests received. We count each individual request received for Apple users/accounts and report the total number of requests received within bands/ranges permissible by law. Pursuant to IP DSI 2018, we are limited to providing this data in bands of 500.

# of Users/Accounts

We count the number of users/accounts in each IPA warrant request received for which Apple has data and report the total number of users/accounts within bands permissible by law. Pursuant to IP DSI 2018, we are limited to providing this data in bands of 500.

Table 9: United States Government National Security Requests January 1–June 30, 2024

Table 9 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	500 - 999	53,000 - 53,499
FISA Content Requests	500 - 999	65,500 - 65,999
National Security Letters	0 - 499	500 - 999

National Security Letters where non-disclosure order lifted	0

National Security Request Type

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

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

# of Requests Received

The number of United States National Security requests received. We count each individual order and National Security Letter received 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 10, 11, 12, 13, 14: United States Government Requests by Legal Process Type January 1–June 30, 2024

Tables 10, 11, 12, 13, and 14 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 10: United States Government Device Requests by Legal Process Type

Table 10 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
12,043	4,649	N/A	52	563	6,779
% of Total (100%)	38.6%	-	~0%	4.7%	56.3%

Table 11: United States Government Financial Identifier Requests by Legal Process Type

Table 11 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
1,341	253	N/A	0	81	1,007
% of Total (100%)	19%	-	-	6%	75%

Table 12: United States Government Account Requests by Legal Process Type

Table 12 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
12,812	6,534	0	141	1,012	5,125
% of Total (100%)	51.0%	0%	1.1%	7.9%	40.0%

Table 13: United States Government Push Token Requests by Legal Process Type

Table 13 provides information regarding the types of legal process Apple received as Push Token Requests.

# of Push Token Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
129	28	N/A	0	52	49
% of Total (100%)	22%	-	0%	40%	38%

Table 14: United States Government Geofence Requests by Legal Process Type

Table 14 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
1	1	N/A	N/A	N/A	N/A
% of Total (100%)	100%	-	-	-	-

# of Device/ Financial Identifier/ Account/ Push Token Requests

The total number of United States government requests Apple received by request type (Device, Financial Identifier, Account, and Push Token). 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/Push Token/Geofence Requests received by Apple.

Table 15: United States Private Party Requests for Information January 1–June 30, 2024

Table 15 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
648	552	32	64
% of Total (100%)	85%	5%	10%

# 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 16: United States Private Party Requests for Account Restriction/Deletion January 1–June 30, 2024

Table 16 provides information regarding United States private party (non-government) requests for Apple account restriction/deletion. Examples of such requests are where private litigants are involved in either civil or criminal proceedings, and requests for Apple to restrict/delete an account may arise. For requests seeking to restrict/delete a customer's Apple ID, Apple requires a court order. Apple complies with these requests insofar as we are legally required to do so.

# of Account Restriction/ Account Deletion Requests Received	# of Accounts Specified in the Requests	# of Requests Rejected/ Challenged Where No Action Taken	# of Account Restriction Requests Where Account Restricted	# of Account Deletion Requests Where Account Deleted
1	1	0	1	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 17: Worldwide Government Digital Content Provider Requests January 1–June 30, 2024

Table 17 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 item, 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[1]	# 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
Asia Pacific				
Australia	2	2	0	0%
China mainland	10	4	6	60%
Hong Kong	3	0	3	100%
Japan	4	3	1	25%
South Korea	1	1	0	0%
Thailand	1	1	0	0%
Asia Pacific Total	21	11	10	48%
Europe, Middle East, India, Africa				
Germany	8	0	8	100%
India	9	3	6	67%
Sweden	1	0	1	100%
Switzerland	1	0	1	100%
Türkiye	2	1	1	50%
Ukraine	1	0	1	100%
Europe, Middle East, India, Africa Total	22	4	18	82%
North America				
Mexico	1	1	0	0%
United States of America	15	1	14	93%
North America Total	16	2	14	88%
Worldwide Total	59	17	42	71%

[1] Only countries / regions where Apple received digital content provider requests during report period January 1–June 30, 2024 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–June 30, 2024

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

Germany - High number of devices specified in requests predominantly due to tax investigations.

Table 2 Worldwide Government Financial Identifier Requests
Japan - High number of financial identifiers specified in requests predominantly due to financial fraud investigations.

Taiwan - High number of financial identifiers specified in requests predominantly due to financial fraud investigations.

Clarifying Lawful Overseas Use of Data (CLOUD) Act Requests
Requests received pursuant to the United States CLOUD Act are included in Apple's transparency report. Apple received 140 CLOUD Act Investigatory Powers Act (IPA) Communications Data Requests (seeking metadata only) issued by the United Kingdom government in this reporting period. We count and report CLOUD Act requests under the country of origin.

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 identified 27 MLAT requests for information 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.