Legal Process Guidelines

Japan & APAC Law Enforcement

These guidelines are provided for use by law enforcement or other government entities in Japan and the Asia Pacific ("APAC") geographical region when seeking information from Apple's relevant entities providing service in the region about users of Apple's products and services or information relating to Apple devices. In these Guidelines, the use of the word "Apple" shall refer to the relevant entity responsible for customer information in a particular region as per Apple's privacy policy http://www.apple.com/legal/privacy/. Apple will update these Guidelines as necessary. This version was released on September 29, 2015.

All other requests for information regarding Apple users, including user questions about disclosure of information, should be directed to https://www.apple.com/privacy/contact/. These Guidelines do not apply to requests that law enforcement agencies make to Apple Inc. or to Apple's relevant local entities outside Japan and the APAC geographical region.

For government information requests, we comply with the laws pertaining to global entities that control our data and we provide details as legally required. For content requests from law enforcement agencies outside the U.S., with the exception of emergency circumstances (defined below in Emergency Requests), Apple will only provide content in response to a search warrant issued pursuant to the Mutual Legal Assistance Treaty process or through other cooperative efforts with the United States Department of Justice.

INDEX

I. General Information

Apple designs, manufactures, and markets mobile communication and media devices, personal computers, and portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV, a portfolio of consumer and professional software applications, the iOS and Mac OS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and Mac App Store. User information is held by Apple in accordance with Apple's privacy policy and the applicable terms of service/terms and conditions for the particular service offering. Apple is committed to maintaining the privacy of the users of Apple products and services. Accordingly, information about users of Apple products and services ("Apple users") will not be released without proper legal process.

The information contained within these Guidelines is devised to provide information to law enforcement agencies in Japan and APAC regarding the legal process that Apple requires in order to disclose electronic information to law enforcement and government agencies in these regions. These Guidelines are not intended to provide legal advice. The frequently asked questions ("FAQ") section of these Guidelines is intended to provide answers to some of the more common questions that Apple receives. Neither these Guidelines nor the FAQ will cover every conceivable circumstance that may arise. Accordingly, law enforcement in Japan should contact japan_police_requests@apple.com and law enforcement agents from countries in APAC should contact apac_police_requests@apple.com with any further questions. These email addresses are intended solely for use by law enforcement and government agents. If you choose to send an email to this address, it must be from a verified law enforcement email address. Nothing within these Guidelines is meant to create any enforceable rights against Apple and Apple's policies may be updated or changed in the future without further notice to law enforcement.

The majority of law enforcement requests that Apple receives seek information regarding a particular Apple device or customer and the specific service(s) that Apple may provide to that customer. Apple can provide Apple device or customer information in so far as Apple still possesses the requested information pursuant to its data retention policies. Apple retains data as outlined in certain "Information Available" sections below. All other data is retained for the period necessary to fulfill the purposes outlined in our privacy policy. Law enforcement should be as narrow and specific as possible when fashioning their requests to avoid misinterpretation and/or objections in response to an overly broad request.

II. Service of Process Guidelines

A. Law Enforcement Information Requests

Apple will accept service of legally valid law enforcement requests by email from law enforcement agencies, provided these are transmitted from the law enforcement agency's verified law enforcement email address. Law enforcement agents in Japan and APAC submitting a legal request to Apple should transmit it directly from their verified law enforcement email address to: japan_police_requests@apple.com for Japan and to apac_police_requests@apple.com for APAC. These email addresses are intended solely for submission of law enforcement requests.

Apple considers a law enforcement legal process document to be valid if it is a Cooperation Letter, a Notice of Obtaining Evidence, subpoena, court order, search and seizure warrant, Australian Telecommunications Act of 1979 Authorization Letter or the local equivalent of these valid legal requests. The type of document required by Apple may vary from country to country and depends on the information sought.

B. Preservation Requests

All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its US data centers. As such, Law enforcement agencies outside the United States seeking such content must obtain legal process through the United States Department of Justice authorities. Where the foreign country has signed a Mutual Legal Assistance Treaty (MLAT) with the United States then appropriate legal process can be obtained through the process specified in the treaty or through other cooperative efforts with the United States Department of Justice authorities. If the preservation of data in advance of impending MLAT process is requested, such request should be submitted to Apple Inc. at subpoenas@apple.com. Please submit preservation requests on law enforcement letterhead with the agent and agency identified within the letter so the request can be verified. Please include an email address and phone number in the letter.

Preservation requests must include the relevant Apple ID/account email address, or full name **and** phone number, and/or full name **and** physical address of the subject Apple account. When a preservation request has been received, Apple will preserve a one-time data pull of the requested existing user data available at the time of the request for 90 days. After this 90 day period, the preservation will be automatically removed from the storage server. However, this period can be extended one additional 90-day period upon a renewed request. More than two preservations for the same account will be treated as requests for an extension of the originally preserved materials, but Apple Inc. will not preserve new material in response to such requests.

C. Emergency Requests

Apple considers a request to be an emergency request when it relates to a circumstance involving a bona-fide immediate and serious threat to:

1) the life/safety of individual(s);
2) the security of a State;
3) commit substantial damage to critical infrastructure or installations.

If the requesting law enforcement officer provides satisfactory confirmation that their request relates to a bona-fide emergency circumstance involving one or more of the above criteria, Apple will examine such a request on an emergency basis.

In order to make an emergency request to Apple, the requesting law enforcement officer should complete the template entitled 'EMERGENCY Law Enforcement Information Request', available at Appendix A, and transmit it directly from their verified law enforcement email address to the mailbox: exigent@apple.com with the words "Emergency Law Enforcement Information Request" in the subject line.

In the event that Apple produces customer data in response to an Emergency Law Enforcement Information Request, a supervisor for the law enforcement agent who submitted the Emergency Law Enforcement Information Request will be contacted and will be asked to confirm to Apple that the emergency law enforcement information request was legitimate. Apple requires that the law enforcement agent who submits the Emergency Law Enforcement Information Request provide the supervisor's contact information upon submission of the request.

In addition, the requesting law enforcement officer could contact Apple's Global Security Operations Center (GSOC) at +1 408-974-2095. When calling GSOC, officers should advise that they have an emergency law enforcement information request, provide brief details of the request, and ask that it be brought to the attention of the appropriate team as an emergency request. This phone number has support for all languages.

D. Account Deletion Requests

In the event that law enforcement is requesting that Apple delete a customer's Apple ID, law enforcement is required to provide Apple with a court order or warrant specifying the account that is to be deleted and the basis for the request.

III. Information Available From Apple

A. Device Registration

Basic registration or customer information, including, name, address, email address, and telephone number is provided to Apple by customers when registering an Apple device prior to iOS 8 and OS Yosemite 10.10. Apple does not verify this information, and it may not be accurate or reflect the device's owner. Registration information for devices running iOS 8 and later versions, as well as Macs running OS Yosemite 10.10 and later versions is received when a customer associates a device to an iCloud Apple ID. This information may not be accurate or reflect the device's owner. Registration information can be obtained with the appropriate legal process document for the requester's country.

Please note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilizes the numbers 0 (zero) and 1 (one) in serial numbers. Requests for serial numbers with either the letter "O" or "I" will yield no results.

B. Customer Service Records

Contacts that customers have had with Apple customer service regarding a device or service may be obtained from Apple. This information may include records of support interactions with customers regarding a particular Apple device or service. Additionally, information regarding the device, warranty, and repair may also be available. This information can be obtained with the appropriate legal process document for the requester's country.

C. iTunes

iTunes is a free software application which customers use to organize and play digital music and video on their computers. It's also a store that provides content for customers to download for their computers and iOS devices. When a customer opens an iTunes account, basic subscriber information such as name, physical address, email address, and telephone number can be provided. Additionally, information regarding iTunes purchase/download transactions and connections, iTunes subscriber information and connection logs with IP addresses can be obtained with the appropriate legal process document for the requester's country.

D. Apple Retail Store Transactions

Point of Sale transactions are cash, credit/debit card, or gift card transactions that occur at an Apple Retail Store. A legally valid request is required to obtain information regarding the type of card associated with a particular purchase, name of the purchaser, email address, date/time of the transaction, amount of the transaction, and store location. When providing a legally valid request requesting Point of Sale records, include the complete credit/debit card number used and any additional information such as date and time of transaction, amount, and items purchased. Additionally, law enforcement may provide Apple with the receipt number associated with the purchase(s) in order

to obtain duplicate copies of receipts, in response to a legally valid request. This information can be obtained with the appropriate legal process document for the requester's country.

E. Apple Online Store Purchases

Apple maintains information regarding online purchases including name, shipping address, telephone number, email address, product purchased, purchase amount, and IP address the purchase. A legally valid request is required in order to obtain this information. When requesting information pertaining to online orders (excluding iTunes purchases), a complete credit/debit card number, an order number, reference number, or serial number of the item purchased. A customer name in combination with these parameters may also be provided, but customer name alone is insufficient to obtain information. This information can be obtained with the appropriate legal process document for the requester's country.

F. iTunes Gift Cards

iTunes gift cards have a sixteen-digit alphanumeric redemption code which is located under the "scratch-off" grey area on the back of the card, and a nineteen-digit code at the bottom of the card. Based on these codes, Apple can determine whether the card has been activated[1] or redeemed as well as whether any purchases have been made on the account associated with the card. When iTunes gift cards are activated, Apple records the name of the store, location, date, and time. When iTunes gift cards are redeemed through purchases made on the iTunes store, the gift card will be linked to a user account. Subscriber information and IP addresses can be available. iTunes Gift Cards purchased through the Apple Online Store can be located in Apple's systems by their Apple Online Store order numbers (note: this only applies to iTunes Gift Cards purchased through Apple as opposed to third-party retailers). This information can be obtained with the appropriate legal process document for the requester's country. Law Enforcement must specify exactly the information that the officer is seeking related to the Gift Card number.

Apple is unable to deactivate iTunes gift cards in response to legal process from a law enforcement/government agency.

G. iCloud

iCloud is Apple's cloud service that allows users to access their music, photos, documents, and more from all their devices. Much of users' digital lives is stored on the cloud as well as on their devices, which is why Apple works so hard to secure users' information across the entire Apple ecosystem. iCloud also enables customers to back up their iOS devices to iCloud. Users can turn off iCloud backup at any time. With the iCloud service, customers can get an iCloud.com email account. iCloud email domains can be @icloud.com, @me.com[2] and @mac.com. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centers.

---

[1] Activated means that the card was purchased at a retail point-of-sale but not that it was used or redeemed (i.e., used to increase the store credit balance on an iTunes account or used to purchase content in the iTunes Store).

[2] iCloud has replaced the MobileMe service. Accordingly, Apple does not have any separate content associated with former MobileMe accounts. If the content is not in iCloud, it is no longer being stored.

iCloud is a subscriber based service. Requests for iCloud data must include the relevant Apple ID/ account email address. If Apple ID/account email address are unknown, Apple requires subscriber information in the form of full name and phone number, and/or full name and physical address to identify the subject Apple account.

The following information may be available from iCloud:

i. Subscriber information

When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud subscriber information and connection logs with IP addresses may be obtained with the appropriate legal process document for the requester's country. Connection logs are retained up to 30 days.

ii. Mail Logs

Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. If an officer seeks specifically Mail Logs, this must be specified in the legal request. This information may be obtained with the appropriate legal process document for the requester's country. iCloud mail logs are retained up to 60 days.

iii. Email Content and Other iCloud Content: PhotoStream, Docs, Contacts, Calendars, Bookmarks, iOS Device Backups

iCloud only stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. iCloud content may include email, stored photos, documents, contacts, calendars, bookmarks and iOS device backups. iOS device backups may include photos and videos in the users' camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centers. Law enforcement agencies outside the United States seeking such content must obtain legal process through the United States Department of Justice authorities. Where the foreign country has signed a Mutual Legal Assistance Treaty (MLAT) with the United States then appropriate legal process can be obtained through the process specified in the treaty or through other cooperative efforts with the United States Department of Justice authorities. Apple Inc. will provide customer content, as it exists in the customer's account, only in response to a search warrant issued pursuant to the MLAT process.

Apple does not retain deleted content once it is cleared from Apple's servers.

H. Find My iPhone

Find My iPhone is a user-enabled feature by which an iCloud subscriber is able to locate his/her lost or misplaced iPhone, iPad, iPod touch or Mac and/or take certain actions, including putting the device in lost mode, locking or wiping the device. More information about this service can be found at http://www.apple.com/icloud/find-my-iphone.html. Location information for a device located through the

Find My iPhone feature is customer facing and Apple does not have records of maps or email alerts provided through the service.

Find My iPhone connection logs may be available and can be obtained with the appropriate legal process document for the requester's country. Find My iPhone connection logs are available for a period of approximately 30 days.

Find My iPhone transactional activity for requests to remotely lock or erase a device may be available if utilized by the customer. Information about remote erase/wipe is available only following receipt of the appropriate legal process document for the requester's country. Apple cannot activate this feature on customers' devices upon a request from law enforcement. The Find My iPhone feature must have been previously enabled by the customer for that specific device. Apple does not have GPS information for a specific device.

I. Extracting Data from Passcode Locked iOS Devices

Requests for technical assistance to access certain content on specified devices should be directed to Apple Inc., via the Mutual Legal Assistance Treaty (MLAT) process. Law enforcement agencies outside the United States seeking such content must obtain legal process through United States Department of Justice authorities. Where the foreign country has signed an MLAT with the United States then appropriate legal process can be obtained through the process specified in the treaty or through other cooperative efforts with the United States Department of Justice authorities.

For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions as data extraction tools are no longer effective. The files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

For iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a search warrant issued pursuant to the MLAT process, Apple Inc. can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ("user generated active files"), can be extracted and provided to law enforcement on external media. Apple Inc. can perform this data extraction process on iOS devices running iOS 4 through iOS 7. Please note that the only categories of user generated active files that can be provided to law enforcement, following receipt by Apple Inc. of a search warrant issued pursuant to the MLAT process, are: SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history. Apple Inc. cannot provide: email, calendar entries, or any third-party App data.

The data extraction process can only be performed at Apple Inc.'s, Cupertino, California headquarters for devices that are in good working order. For Apple Inc. to assist in this process, the language outlined below must be included in a search warrant , and the search warrant must include the serial or IMEI number of the device. For more information on locating the serial or IMEI number of an iOS device, refer to: http://support.apple.com/kb/ht4061.

Please make sure that the name of the judge on the search warrant is printed clearly and legibly in order for the paperwork to be completed.

Once law enforcement has obtained a search warrant containing this language, it may be served on Apple Inc. by email to subpoenas@apple.com. The iOS device can be provided to Apple Inc. for data extraction either through an in-person appointment or through shipment. If law enforcement chooses to ship the device, the device should not be shipped unless and until the officer receives an email from Apple requesting shipment.

For an in-person data extraction process, Apple requires that the law enforcement agent bring a FireWire hard drive with a storage capacity of at least two times the memory capacity for the iOS

device. Alternatively, if law enforcement chooses to ship the device, law enforcement should provide Apple with an external hard drive or USB "thumb" drive with a storage capacity of at least two times the memory capacity for the iOS device. Please do not send the device unless and until you receive an email requesting its shipment.

After the data extraction process has been completed, a copy of the user generated content on the device will be provided. Apple Inc. does not maintain copies of any user data extracted during the process; accordingly all evidence preservation remains the responsibility of the law enforcement agency.

Required Search Warrant Language:

> "It is hereby ordered that Apple Inc. assist [LAW ENFORCEMENT AGENCY] in its search of one Apple iOS device, Model #_____, on the _____ network with access number (phone number) _____, serial[3] or IMEI[4] number _____, and FCC ID#_____ (the "Device"), by providing reasonable technical assistance in the instance where the Device is in reasonable working order and has been locked via passcode protection. Such reasonable technical assistance consists of, to the extent possible, extracting data from the Device, copying the data from the Device onto an external hard drive or other storage medium, and returning the aforementioned storage medium to law enforcement. Law Enforcement may then perform a search of the device data on the supplied storage medium.
>
> It is further ordered that, to the extent that data on the Device is encrypted, Apple may provide a copy of the encrypted data to law enforcement but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data.
>
> Although Apple shall make reasonable efforts to maintain the integrity of data on the Device, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents."

J. Other Available Device Information

MAC Address: A Media Access Control address (MAC address), is a unique identifier assigned to network interfaces for communications on the physical network segment. Any Apple product with network interfaces will have one or more MAC addresses, such as Bluetooth, Ethernet, Wi-Fi, or FireWire. By providing Apple with a serial number (or in the case of an iOS device, IMEI, MEID, or UDID), the MAC address can be obtained with the appropriate legal process document for the requester's country.

UDID: The unique device identifier (UDID) is a sequence of 40 letters and numbers that is specific to a particular iOS device. It will look similar to the following: 2j6f0ec908d137be2e1730235f5664094b831186.

---

[3]Note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilizes the numbers 0 (zero) and 1 (one) in serial numbers. iOS extractions for serial numbers with either the letter "O" or "I" can not be performed.

[4] The IMEI number is engraved on the back of cellular iPads, the original iPhone, iPhone 5, 5c, 5s, 6, and 6 Plus. For more information, see http://support.apple.com/kb/ht4061. Note that for models with IMEI numbers engraved on the SIM tray, the SIM tray in the device may not be the matching original that came with the device.

If law enforcement is in possession of the device, the device may be connected to iTunes in order to obtain the UDID. Under the iTunes summary tab, the UDID can be revealed by clicking on the serial number.

K. Requests for Apple Retail Store Surveillance Videos

Video surveillance records are maintained at an Apple retail store for a maximum of thirty days. After this time frame has passed, video surveillance may not be available. A request from law enforcement for video surveillance can be made via email to japan_police_requests@apple.com for Japan and to apac_police_requests@apple.com for greater APAC. Once the request is received, it will be forwarded to the appropriate team for processing. If there is responsive data, that team will contact the law enforcement agent directly.

L. Game Center

Game Center is Apple's social gaming network. Information regarding Game Center connections for a user or a device may be available. Connection logs with IP addresses, and transactional records can be obtained with the appropriate legal process document for the requester's country.

M. iOS Device Activation

When a customer activates an iOS device or upgrades the software, certain information is provided to Apple from the service provider or from the device, depending on the event. IP addresses of the event, ICCID numbers, and other device identifiers may be available. This information can be obtained with the appropriate legal process document for the requester's country.

N. Sign-on Logs

Sign-on activity for a user or a device to Apple services such as iTunes, iCloud, My Apple ID, and Apple Discussions, when available, may be obtained from Apple. Connection logs with IP addresses or sign-on transactional records can be obtained with the appropriate legal process document for the requester's country.

O. My Apple ID and iForgot Logs

My Apple ID and iForgot logs for a user may be obtained from Apple. My Apple ID and iForgot logs may include information regarding password reset actions. Connection logs with IP addresses or transactional records can be obtained with the appropriate legal process document for the requester's country.

P. FaceTime

FaceTime communications are end-to-end encrypted and Apple has no way to decrypt FaceTime data when it is in transit between devices. Apple cannot intercept FaceTime communications. Apple has FaceTime call invitation logs when a FaceTime call invitation is initiated. These logs do not indicate that any communication between users actually took place. Apple has no information as to whether the FaceTime call was successfully established or duration of a FaceTime call. FaceTime call invitation logs are retained up to 30 days. FaceTime call invitation logs can be obtained with the appropriate legal process document for the requester's country.

IV. Frequently Asked Questions

Q: Can I contact Apple with questions regarding my law enforcement information request or legal process?

A: Yes, all questions or inquiries should be emailed to japan_police_requests@apple.com for Japan and to apac_police_requests@apple.com for the APAC region.

Q: Can Apple provide me with the passcode of an iOS device that is currently locked?

A: No, Apple does not have access to a user's passcode but, depending on the versions of iOS the device is running, may be able to extract some data from a locked device with a valid search warrant issued pursuant to the MLAT process, as described in the Guidelines.

Q: Does Apple store GPS information that can be provided in response to requests?

A: No, Apple does not track geolocation of devices.

Q: What should be done with response information when law enforcement has concluded the investigation/criminal case using it?

A: Apple requires that any files and records produced for law enforcement that contain personally identifiable information (including any copies made) must be destroyed after the related investigation, criminal case, and all appeals have been fully exhausted.

Q: Can you help me return a stolen or lost device to the rightful owner?

A: In cases where law enforcement has recovered a suspected lost or stolen device and are seeking to return it to the "original owner," law enforcement should forward a request for registration information via email to: japan_police_requests@apple.com for Japan and apac_police_requests@apple.com for APAC. Please include the device's serial or IMEI number and any additional relevant information. If registration information is available, it will be provided so that law enforcement can contact the registrant and advise him or her of the recovered device.

V. Appendix A

The EMERGENCY Law Enforcement Information Request form is available as an editable PDF at:
http://www.apple.com/legal/privacy/le-emergencyrequest.pdf