Legal Process Guidelines

U.S. Law Enforcement

These Guidelines are provided for use by law enforcement or other government entities in the U.S. when seeking information from Apple Inc. ("Apple") about users of Apple's products and services, or from Apple devices. Apple will update these Guidelines as necessary. This version was released on September 17, 2014.

All other requests for information regarding Apple users, including user questions about disclosure of information, should be directed to http://www.apple.com/privacy/contact/. These Guidelines do not apply to requests that law enforcement agencies make outside the U.S. to Apple's relevant local subsidiaries.

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 ("Apple users"). Accordingly, information about 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 regarding the legal process that Apple requires in order to disclose electronic information to law enforcement and government agencies. 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, please contact subpoenas@apple.com with any further questions. This email address is intended strictly for use by law enforcement and government agents. If you choose to send an email to this address, it must be from a valid government 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 subpoenas, search warrants, and court orders 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. Law enforcement should be as narrow and specific as possible when fashioning their legal process to avoid misinterpretation and/or objections in response to an overly broad request. Law enforcement is required to obtain a search warrant that is issued upon a probable cause showing for search warrants requesting user content.

II. Service of Process Guidelines

A. Service of Law Enforcement Subpoenas, Search Warrants, and Court Orders

Apple will accept service of subpoenas, search warrants, and court orders for information by fax or mail from law enforcement agencies.

Please direct service via fax to:

Fax Number: (408) 974-9316

Apple Inc.
Attention: Privacy and Law Enforcement Compliance
1 Infinite Loop, Cupertino, CA 95014

We require law enforcement to include the following information with the legal request so the request can be verified:

Law Enforcement Agency
Law Enforcement Agent Name and Badge/ID number
Agency issued email address
Law Enforcement Phone number (with extension if applicable)
Verifiable physical return address
Law Enforcement Fax number

Note: All matters that are not law enforcement related must be either personally served at Apple's headquarters in Cupertino, California or served through CT Corporation (Apple's registered agent for service of process). For any inquiries related to law enforcement legal process, please contact: subpoenas@apple.com or Apple's Subpoena Hotline at (408) 974-8100. If you are inquiring regarding the status of a specific subpoena, search warrant, or court order, please do not contact Apple until at least 10 business days after service of your request unless the matter involves imminent harm or threat to life.

B. Witness Testimony Subpoenas

Apple will not waive service requirements for subpoenas seeking witness testimony nor accept service via fax. All subpoenas seeking witness testimony must either be personally served on Apple or served through Apple's registered agent for service of process. Apple will resist subpoenas for witness testimony that are served with fewer than 14 days advance notice.

C. Preservation Requests

Requests to preserve information pursuant to 18 U.S.C. § 2703(f) should be directed to Apple's Privacy and Law Enforcement Compliance Group by fax to (408) 974-9316. Please submit preservation requests on law enforcement letterhead with the agent and agency identified within the letter and include a valid government email address and phone number in the letter so the request can be verified.

Preservation requests must include the email address, or full name and phone number, 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 by 90 days upon a renewed preservation request. More than two preservations for the same account will be treated as requests for an extension of the originally preserved materials, but Apple will not preserve new material in response to such requests.

D. Emergency Disclosure

Under 18 U.S.C. §§ 2702(b)(7) and 2702(c)(4) Apple is permitted, but not required, to voluntarily disclose information, including contents of communications and customer records, to a federal, state, or local governmental 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. In order to request that Apple voluntarily disclose information on an emergency basis, please fill out the Emergency Disclosure Form attached as Appendix A and send a copy of the completed form by email to subpoenas@apple.com and include "Emergency Disclosure Request" in the subject line. Alternatively, the completed form may be submitted by fax to (408) 974-9316.

If you need to contact Apple after hours (before 8:00 am or after 5:00 pm Pacific time) for an emergency inquiry, please contact Apple's Global Security Operations Center (GSOC) at (408) 974-2095.

E. User Notice

Apple will notify its customers when their personal information is being sought in response to legal process except where providing notice is prohibited by the legal process itself, by a court order Apple receives (e.g., an order under 18 U.S.C. §2705(b)), or by applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or in situations where the case relates to child endangerment.

Apple will provide delayed notice for emergency disclosure requests except where notice is prohibited by court order or applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or in situations where the case relates to child endangerment.

III. Information Available From Apple

A. Device Registration Information

Basic registration or customer information, including, name, address, email address, and telephone number is provided to Apple by customers when registering an Apple device. Apple does not verify this information, and it may not be accurate or reflect the device's owner. Additionally, the date of registration, purchase date and device type may also be included. This information can be obtained with a subpoena or greater legal process.

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 a subpoena or greater legal process.

C. iTunes Information

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, update/re-download connections, and iTunes Match connections may also be available. iTunes subscriber information and connection logs with IP addresses can be obtained with a subpoena or greater legal process. iTunes purchase/download transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal

standard. A search warrant issued upon a showing of probable cause is required for Apple to provide the specific content purchased or downloaded.

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 subpoena or greater legal process 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 legal process 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 subpoena or greater legal process.

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 of where a purchase was made. A subpoena or greater legal process 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, serial number of the item purchased, and/or customer name is required.[1]

F. iTunes Gift Cards

iTunes gift cards have a sixteen-digit alphanumeric redemption code which is located under the "scratch-off" gray 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[2] or redeemed as well as whether any purchases have been made 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. iTunes gift cards purchased through the Apple Online Store can be located in Apple 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). Information

---

[1] If law enforcement provides only a name and not the information described above, responsive information cannot be obtained.

[2] 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).

regarding the customer who redeemed the cards will require a subpoena, and transactional information about iTunes purchases made with the card will require a court order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard. A search warrant issued upon a showing of probable cause is required for Apple to provide the specific content purchased.

G. iCloud

iCloud is Apple's cloud service that allows users to access their music, photos, documents, and more from all their devices. iCloud also enables subscribers to back up their iOS devices to iCloud. With the iCloud service, subscribers can set up an iCloud.com email account. iCloud email domains can be @icloud.com, @me.com[3] and @mac.com. iCloud data is encrypted wherever an iCloud server is located. 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. 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 can be obtained with a subpoena or greater legal process.

ii. Mail Logs

iCloud mail logs are retained for approximately a period of 60 days. Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs may be obtained with a court order under 18 U.S.C. § 2703(d) or a court order with an equivalent legal standard or a search warrant.

iii. Email Content

iCloud only stores the email a subscriber has elected to maintain in the account while the subscriber's account remains active. Apple is unable to provide deleted content.

---

[3] 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.

Available email content may be provided in response to a search warrant issued upon a showing of probable cause.

iv. Other iCloud Content. Photo Stream, 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. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include 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. iCloud content may be provided in response to a search warrant issued upon a showing of probable cause.

H. Find My iPhone

Finding 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 locking or wiping the device. More information about this service can be found at http://www.apple.com/icloud/. Location information for a device located through the Find My iPhone feature is user 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 a subpoena or greater legal process. Find My iPhone transactional activity for requests to remotely lock or erase a device may be available with an order under 18 U.S.C. § 2703(d) or a court order with the equivalent legal standard or a search warrant.

Apple cannot activate this feature on users' devices upon a request from law enforcement. The Find My iPhone feature has to have been previously enabled by the user for that specific device. Apple does not have GPS information for a specific device or user.

I. Extracting Data from Passcode Locked iOS Devices

For all devices running iOS 8.0 and later versions, Apple will no longer be performing iOS data extractions as the data sought will be encrypted and Apple will not possess the encryption key.

For iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant issued upon a showing of probable cause, Apple 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 can perform this data extraction process on iOS devices running iOS 4 through iOS 7. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant to a valid search warrant, are: SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party app data.

The data extraction process can only be performed at Apple's Cupertino, California headquarters for devices that are in good working order. For Apple 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 IMEI and serial 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 by fax to (408) 974-9316. The iOS device can be provided to Apple for data extraction either through an in person appointment or through shipment. However, Apple recommends that law enforcement attend the data extraction. 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 that is capable of storing the equivalent of two times the memory size of 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 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 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), this information may be obtained with a subpoena or greater legal process.

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 following: 2j6f0ec908d137be2e1730235f5664094b831186.

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.

---

[4] The IMEI number is engraved on the back of cellular iPads, the original iPhone, iPhone 5, 5c, and 5s. 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.

K. Requests for Apple Retail Store Surveillance Videos

Video surveillance records may vary by store location. Video surveillance records are typically maintained at an Apple store for approximately thirty days. After thirty days, video surveillance may no longer be available. A request for video surveillance can be made at any local Apple retail store. Law enforcement should provide specific date, time, and related transaction information regarding the video requested.

L. Game Center Information

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 can be obtained with a subpoena or greater legal process. Game Center transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard. A search warrant issued upon a showing of probable cause is required for Apple to provide the specific game(s) played.

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 a subpoena or greater legal process.

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 can be obtained with a subpoena or greater legal process. Sign-on transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard or search warrant.

O. Password Activity Logs

Apple ID password activity logs for a user may be obtained from Apple. Information regarding password activity actions including password reset information for a user may be available. Connection logs with IP addresses can be obtained with a subpoena or greater legal process. Password activity transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard or search warrant.

IV. Frequently Asked Questions

Can I email or call Apple with questions regarding my legal process?

Yes, questions or inquiries regarding government legal process can be emailed to subpoenas@apple.com or please call (408) 974-8100.

I need to personally serve Apple, where should I go?

All personal service can be made at Apple's Cupertino, California headquarters located at the following address:

Apple Inc.
1 Infinite Loop
Cupertino, CA 95014-2084

Can I serve a deposition subpoena directly on an Apple retail store?

No, all subpoenas for testimony, including subpoenas for deposition or trial testimony, need to be personally served on Apple.

I requested information on my fax cover sheet, why was it not provided?

Requests for information not included within the body of the signed subpoena, search warrant, or court order will be disregarded; all information requested must be in the actual executed legal process document.

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

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

Does a device have to be registered with Apple in order to function?

No, a device does not have to be registered with Apple in order for it to function or be used.

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

In cases where law enforcement has recovered a lost or stolen device and wants to return it to the "original owner," contact Apple Customer Care (ACC) via email at law_enforcement_esc@apple.com. Please include the device's serial number in your email and any additional pertinent information. If registration information is available, ACC will contact the owner and instruct him or her to contact law enforcement to recover the device. A subpoena is not required in most cases. However, if there is conflicting information located within our databases you may be instructed to submit a subpoena.

How will the information requested be delivered?

Responsive production of records and information will be sent in an encrypted electronic container via email or, in some instances, via FedEx delivery. If no responsive information is available, a letter indicating this will be sent via email or, in some cases, via U.S. mail.

I am looking into whether a user's email reach the requirements for interstate commerce. Where are the iCloud email servers located?

Apple's U.S. email servers are located in California, Nevada, and North Carolina.

Does Apple store GPS information that can be produced under proper legal process?

No, Apple does not track geolocation of devices.

What should be done with the produced files and records when law enforcement has concluded the investigation/criminal case?

Apple requires that any information and data provided to law enforcement containing personally identifiable information (including any copies made) must be destroyed after the related investigation, criminal case, and all appeals have been fully exhausted.

Do you notify users of criminal legal process?

Yes, unless there is a non-disclosure order or applicable law prohibiting notice, or we believe in our sole discretion that such notice may pose immediate risk of serious injury or death to a member of the public or the case relates to a child endangerment matter.

Can Apple intercept users' communications pursuant to a Wiretap Order?

Apple can intercept users' 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. Mail header data may be provided in response to a valid Pen Register Order that includes a showing issued upon 18 U.S.C. § 2703(d) of specific and articulable facts showing that there are reasonable grounds to believe that the records and information sought are relevant and material to an ongoing criminal investigation.

V. Appendix A

As per section II (D) above, to request that Apple voluntarily disclose information on an emergency basis, please fill out the Emergency Disclosure Form and submit it via email to subpoenas@apple.com with "Emergency Disclosure Request" included in the email subject. Alternatively, the completed form may be submitted by fax to (408) 974-9316.

Apple Emergency Disclosure Request Form for Law Enforcement

Please provide the information requested below in order to assist Apple in exercising its discretion to disclose under the standard stated in 18 USC § 2702(b)(8) and § 2702(c)(4). Please email this form to subpoenas@apple.com with the subject line: Emergency Disclosure Request. Please note that it is Apple's policy to notify a customer when we receive an emergency request from law enforcement requesting customer account information 90 days after the request is received.

1. What is the nature of the emergency involving death or serious physical injury?

2. Whose death or serious physical injury is threatened?

3. When did this emergency arise and when did you become aware of it?

4. Why is this situation an emergency such that normal disclosure processes would be insufficient or not timely? Is there reason to believe the threat is imminent? Please provide information that suggests that there is a specific deadline before which it is necessary to receive the requested information.

5. What specific information do you believe is in Apple's possession related to the emergency? Please make your request as narrow as possible; requesting all information about an account will delay the processing of your request. NOTE: You must specify the Device ID or an email address associated with an Apple iTunes or iCloud account.

6. Please explain how the information you are requesting will assist in averting the threatened emergency.

This form has been completed by an authorized law enforcement official.
I declare under penalty of perjury that the foregoing is true and correct.

_____ _____

Signature of requesting law enforcement agent *Date*

_____ _____

Printed name of requesting law enforcement agent *Badge/ID number of requesting agent*

_____ _____

Contact email address of law enforcement agent *Direct contact telephone number*

_____

Law enforcement agency