



# Legal Process Guidelines

## EMEIA Law Enforcement

These guidelines are provided for use by law enforcement or other government entities in the EMEIA (Europe, Middle East, India, Africa) geographical region when seeking information from Apple's relevant entities providing service in the region about users of Apple's products and services or from Apple devices. In these Guidelines, Apple shall mean the relevant subsidiary responsible for customer information in a particular region as per our privacy policy at <http://www.apple.com/legal/privacy/en-ww/>. Apple will update these Guidelines as necessary. This version was released on [Day] [Month], 2014.

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 subsidiaries outside the EMEIA geographical region.

### INDEX

#### I. General Information

#### II. Service of Process

- A. Law Enforcement Information Requests
- B. Preservation Requests
- C. Emergency Requests
- D. User Notice

#### III. Information Available From Apple

- A. Device Registration Information
- B. Customer Service Records
- C. iTunes Information
- D. Retail Store Transactions
- E. Apple Online Store Purchases
- F. iTunes Gift Cards
- G. iCloud
- H. Find My iPhone
- I. Extracting Data from Passcode Locked iOS Devices
- J. Other Available Device Information
- K. Requests for Apple Retail Store Surveillance Videos
- L. Game Center Information
- M. iOS Device Activation
- N. Sign-on Logs
- O. Password Activity Logs

#### IV. Frequently Asked Questions

V. Appendix A

VI. Appendix B

## 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 in EMEA regarding the legal process that Apple requires in order to disclose electronic information to law enforcement and government agencies in EMEA. 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 [law.enf.emeia@apple.com](mailto:law.enf.emeia@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 law enforcement/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 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. 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 information requests by email from law enforcement agencies, provided these are transmitted from the official email address of the law enforcement agency concerned. Law enforcement officers in EMEA wishing to make an information request to Apple should complete a Law Enforcement Information Request template (as provided at Appendix A) and transmit it directly from their official law enforcement email address to the mailbox: [law.enf.emeia@apple.com](mailto:law.enf.emeia@apple.com) This email address is intended strictly for submission of law enforcement requests.

Apple considers a law enforcement information request to be legally valid if it is made in circumstances pertaining to the bona-fide prevention, detection or investigation of offences and will respond appropriately to what it considers to be such legally valid requests.

### B. Preservation Requests

All content data is encrypted wherever a 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. 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 fax number: +1 408-974-9316. 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 so the request can be verified.

When a preservation request has been received, Apple Inc. 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 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 for EMEIA Geographical Region', as attached at Appendix B, and transmit it directly from their official law enforcement email address to the mailbox: [law.enf.emeia@apple.com](mailto:law.enf.emeia@apple.com), with the words "Emergency Request" in the subject line.

In addition, the requesting law enforcement officer should contact Apple's Global Security Operations Centre (GSOC) at +1 408-974-2095, 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. User Notice**

Apple will notify its customers when their personal information is being sought in a legally valid law enforcement information request except where it reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice.

## **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 legally valid request.

## **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 legally valid request.

## **C. iTunes Information**

iTunes is a free software application which customers use to organise 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 legally valid request.

iTunes purchase/download transactional records are controlled by iTunes S.à.r.l., which is a Luxembourg company. Due to legislative provisions, iTunes can only respond to requests such as this when they have been validated by the Public Prosecutor of Luxembourg and forwarded to iTunes for response. Requests for these records should be submitted to the Public Prosecutor of Luxembourg at the following address: Parquet Général, Procureur Général d'Etat, Cité Judiciaire Bât. CR, Plateau du St Esprit, L-2080 LUXEMBOURG, fax number: +352 47 05 50, email : [parquet.general@justice.etat.lu](mailto:parquet.general@justice.etat.lu)

## **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.

## **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 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, serial number of the item purchased, and/or customer name is required.<sup>1</sup>

## **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

---

<sup>1</sup> If law enforcement provides only a name and not the information described above, responsive information cannot be obtained.

card. Based on these codes, Apple can determine whether the card has been activated<sup>2</sup> 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 regarding the customer who redeemed the cards will require a legally valid request, and information about online iTunes store purchases made with the card will require a request to be submitted to the Public Prosecutor of Luxembourg at the following address: Parquet Général, Procureur Général d'Etat, Cité Judiciaire Bât. CR, Plateau du St Esprit, L-2080 LUXEMBOURG, fax number: +352 47 05 50, email : [parquet.general@justice.etat.lu](mailto:parquet.general@justice.etat.lu)

## 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<sup>3</sup> 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 legally valid request.

### 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. This information is available only following receipt of a legally valid request.

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

iCloud only stores the email a subscriber has elected to maintain in the account while the subscriber's account remains active. 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 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. This 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. Law enforcement agencies outside the United States seeking such content must obtain legal process

---

<sup>2</sup> 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).

<sup>3</sup> 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.

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 subscriber content, as it exists in the subscriber'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 locking or wiping the device. More information about this service can be found at <http://www.apple.com/icloud/features/#fmip>. 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 legally valid request. Find My iPhone transactional activity for requests to remotely lock or erase a device may be available only following receipt of a legally valid request.

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

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 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 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 fax at +1 408-974-9316. The iOS device can be provided to Apple Inc. for data extraction either through an in-person appointment or through shipment. However, Apple Inc. 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.

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 or IMEI<sup>4</sup> 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 legally valid request.

**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.

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.

---

<sup>4</sup> 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 maintained at an Apple retail store for a maximum of thirty days. In many jurisdictions in Europe it is as short as two days taking account of local laws. After this time frame has passed, video surveillance may not be available. A request from law enforcement 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 and transactional records are available only following receipt of a legally valid request.

## **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 is available only following receipt of a legally valid request.

## **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 and transactional records are available only following receipt of a legally valid request.

## **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 and transactional records are available only following receipt of a legally valid request.

## 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: [law.enf.emeia@apple.com](mailto:law.enf.emeia@apple.com).

**Q: Does a device have to be registered with Apple in order to function or be used?**

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

**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 version of iOS that 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: What should be done with response information when law enforcement has concluded the investigation/criminal case?**

A: Apple requires that any information and data produced for 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.

**Q: Do you notify users of receiving law enforcement information requests in relation to them?**

A: Yes, Apple will send notice to the user(s) concerned when their personal information is being sought in a legally valid law enforcement information request except where it reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice.

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

A: In cases where you as law enforcement in EMEIA have recovered a suspected lost or stolen device and want to return it to the "original owner," you should forward a request to our mailbox: [law.enf.emeia@apple.com](mailto:law.enf.emeia@apple.com) and include the device's serial or IMEI number and any additional relevant information. If registration information is available, we will contact the registrant and advise him or her to contact you.

## V. APPENDIX A

This form is also available as a separate PDF at <http://www.apple.com/legal/privacy/emeia-le-inforequest.pdf>

Law Enforcement Information Request for EMEA Geographical Region	
Law Enforcement Agency	Name:
	Country:
	Location:
Requesting Officer	Name and Rank:
	Email:
	Phone:
Case Context	Case Type & Reference Number:
	Case Occurred Date & Location:
	Case Overview:
Information Context	Purpose for which information is requested and legal basis on which it is believed that the information can be requested:
	Information provided to support request:
	Information Requested:

## VI. APPENDIX B

This form is also available as a separate PDF at <http://www.apple.com/legal/privacy/emeia-le-emergencyrequest.pdf>

EMERGENCY Law Enforcement Information Request for EMEIA Geographical Region	
Law Enforcement Agency	Name:
	Country:
	Location:
Requesting Officer	Name and Rank:
	Email:
	Phone:
Case Context	What is the nature of the emergency involving 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.
	Please provide the name(s) of the individual(s) whose life/safety is threatened; or the name of the State whose security is threatened; or the name(s) of the critical infrastructure(s) or installation(s) to which substantial damage is threatened:
	When did this emergency arise and when did you become aware of it:

**EMERGENCY Law Enforcement Information Request  
for EMEA Geographical Region**

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

**Information Context**

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. You must specify the Device ID or an email address associated with an Apple iTunes or iCloud account. NOTE: 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.

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