



法律程序指南

美国境外的政府和执法机构

本指南面向美国境外的政府和执法机构提供，后者在相关国家或地区请求 Apple 实体提供关于使用 Apple 设备、产品和服务的顾客的信息时，应该遵循本指南。Apple 在必要时将更新本指南。

在本指南中，“Apple”指的是在特定地区或国家对顾客信息负责任的相关实体。Apple 作为一家全球性的公司，在不同的司法辖区设有多个法律实体，这些实体将对他们收集的个人信息负责，并由他们代表 Apple Inc. 处理此类个人信息。例如，美国境外的 Apple 零售店实体中的销售点信息将由各个国家/地区的各个 Apple 零售店实体控制。根据具体辖区内各项服务相关条款的具体规定，与 Apple Store 在线商店和 Apple 媒体服务相关的个人信息可能也会由美国境外的法律实体控制。通常，Apple 在美国境外的法律实体 (澳大利亚、加拿大、爱尔兰和日本) 负责其各自所在地区内的 Apple 服务相关顾客数据。

所有其他关于 Apple 顾客信息的请求，包括关于信息披露事宜的顾客问题，都应该参阅 <https://www.apple.com.cn/privacy/contact/>。本指南不适用于美国政府和执法机构向 Apple Inc. 提出的请求。

对于政府和执法机构提出的信息请求，Apple 遵守适用于数据控制的全球各实体的法律，并且我们会在法律要求时提供详细信息。美国境外的政府和执法机构在提出任何内容请求时，都必须遵守包括美国《电子通讯隐私法》(United States Electronic Communications Privacy Act, 以下简称“ECPA”) 在内的适用法律，但紧急情况 (详见下文“紧急请求”中的定义) 除外。如果一方根据《法律互助条约》(Mutual Legal Assistance Treaty) 或《澄清境外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act) 下的行政协议 (以下简称“CLOUD 法案协议”) 提出请求，则符合 ECPA 的规定。Apple 仅在回应此类合法有效的流程时才会提供顾客内容，因为该内容存储在顾客的帐户中。

另外，根据中国的法律要求，对于将国家或地区设置为“中国”的 Apple ID，其 iCloud 服务的运营已转移至贵州，由云上贵州大数据产业发展有限公司 (以下简称“GCBD”) 管理。因此，自 2018 年 2 月 28 日起，与此类顾客相关的 iCloud 数据请求应通过以下电子邮件地址发送至 GCBD：china_police_requests@gzdata.com.cn。

对于私人机构请求，Apple 遵守控制顾客数据并按法律要求提供数据的当地实体有关的法律。

Apple 提供了一个集中处理流程，用于接收、跟踪、处理和回应政府、执法机构和私人机构提出的合法的法律请求，涵盖从收到请求到提供回应的整个过程。我们法律部门中一支训练有素的团队，将负责审核和评估收到的所有请求，如果 Apple 确定请求缺乏有效的法律依据，或者认为请求不明确、不恰当或过于宽泛，则会质疑或拒绝该请求。

索引

I. 一般信息

II. 向 Apple 提出的法律请求

- A. 政府和执法机构信息请求
- B. 管理并回应政府和执法机构信息请求
- C. 保留请求
- D. 紧急请求
- E. 帐户限制/删除请求
- F. 顾客通知

III. Apple 可以提供的信息

- A. 设备注册
- B. 顾客服务记录
- C. Apple 媒体服务
- D. Apple Store 零售店交易
- E. Apple Store 在线商店购买交易
- F. 礼品卡
- A. Apple Pay
- G. iCloud
- H. “查找”
- I. 从密码锁定的 iOS 设备中提取数据
- J. 其他可提供的设备信息
- K. Apple Store 零售店闭路电视数据请求
- L. Game Center
- M. iOS 设备激活
- N. 连接日志
- O. “我的 Apple ID”和 iForgot 日志
- P. FaceTime 通话
- Q. iMessage 信息
- S. Apple TV app
- T. 通过 Apple 登录

IV. 常见问题解答

I. 一般信息

Apple 设计、制造和营销移动通信和媒体设备、个人电脑、便携式数字音乐播放器，并销售各种相关软件、服务、外围设备、网络解决方案和第三方数字内容和应用程序。Apple 的产品和服务包括 Mac、iPhone、iPad、iPod touch、Apple TV、Apple TV+、Apple Watch、HomePod、AirPods、各种消费类和专业软件应用程序、iOS 和 Mac OS X 操作系统、iCloud 以及各种配件、服务和支持产品。Apple 还通过 Apple Music、App Store、Apple Books 和 Mac App Store 销售和提供数字内容和应用程序。对于特定服务，Apple 根据 Apple 的[隐私政策](#)和适用的[服务条款](#)保留顾客信息。Apple 致力于维护使用 Apple 产品和服务的顾客（以下简称“Apple 顾客”）的隐私。因此，除了法律规定的紧急情况外，未经有效的法律程序，关于 Apple 顾客的信息不会予以提供。

Apple 在向美国境外的政府和执法机构提供电子信息时，要求经过法律程序，本指南中包含的信息旨在为美国境外的政府和执法机构提供关于这些法律程序的信息。本指南的目的不是提供法律建议。本指南的常见问题解答（下称“FAQ”）部分旨在回答 Apple 遇到的一些比较常见的问题。无论是本指南还是 FAQ，都不会涵盖所有可以想到的可能出现的情况。

如有其他疑问，请联系 lawenforcement@apple.com。

上述邮箱仅限政府和执法机构人员使用。如果你选择向以上邮箱发送电子邮件，则应该通过有效的政府官方电子邮件地址或执法机构官方电子邮件地址发送。

向 Apple 提出的法律请求应该寻求特定 Apple 设备或顾客的相关信息，以及 Apple 可能向该顾客提供的具体服务。只要 Apple 根据其数据保留政策仍然保有所请求的信息，Apple 就可以提供 Apple 设备或顾客信息。Apple 会保留在下面特定的“可提供信息”部分中所列的数据。所有其他数据将按照我们[隐私政策](#)中所述目的保留相应的一段时间。政府和执法机构在提出请求时应尽可能缩小范围并具体化，以免不明确、不恰当或过于宽泛的请求遭到误解、反对、质疑和/或拒绝回应。美国境外的政府和执法机构在提出任何内容请求时，都必须遵守包括美国《电子通讯隐私法》(United States Electronic Communications Privacy Act，以下简称“ECPA”) 在内的适用法律，但紧急情况（详见下文“紧急请求”中的定义）除外。如果一方根据《法律互助条约》(Mutual Legal Assistance Treaty) 或《澄清境外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act) 下的行政协议（以下简称“CLOUD 法案协议”）提出请求，则符合 ECPA 的规定。Apple 仅在回应此类合法有效的流程时才会提供顾客内容，因为该内容存储在顾客的帐户中。

另外，根据中国的法律要求，对于将国家或地区设置为“中国”的 Apple ID，其 iCloud 服务的运营已转移至贵州，由云上贵州大数据产业发展有限公司（以下简称“GCBD”）管理。因此，自 2018 年 2 月 28 日起，与此类顾客相关的 iCloud 数据请求应通过以下电子邮件地址发送至 GCBD：china_police_requests@gzdata.com.cn。

本指南中的内容不构成任何可将 Apple 作为执行对象的权利，Apple 的政策将来可能会更新或有所变动，恕不另行通知政府部门或执法机构。

II. 向 Apple 提出的法律请求

A. 政府和执法机构信息请求

Apple 接受政府部门或执法机构通过电子邮件发送其提出的合法有效的信息请求，前提是这些电子邮件是从相关政府部门或执法机构的官方电子邮件地址发出的。美国境外的政府部门和执法机构人员在向 Apple 提交信息请求时，应填写

[政府部门和执法机构信息请求模板](#)，然后通过政府部门或执法机构的官方电子邮件地址将该模板直接发送至 lawenforcement@apple.com。

上述邮箱仅限政府和执法机构人员使用。如果请求涉及五个或更多标识符，例如设备序列号/IMEI 编号、Apple ID、

电子邮件地址或发票/订单编号，则这些标识符应该以可编辑的格式 (例如：Numbers 表格、Pages 文稿等) 进行发送。通常在进行与设备、帐户或财务交易相关信息的搜索时需要用到此类标识符。

如需 Apple 披露顾客信息，作为对执法机构所提出请求的响应，提出请求的执法人员有必要说明授权执法机构从数据控制方 (例如 Apple) 以个人数据形式收集证据类信息的法律依据。例如，以下均属于 Apple 认为合法有效的请求：Production Orders (澳大利亚、加拿大、新西兰)、Requisition or Judicial Rogatory Letters (法国)、Solicitud Datos (西班牙)、Ordem Judicial (巴西)、Auskunftersuchen (德国)、Obligation de dépôt (瑞士)、個人情報の開示依頼 (日本)、Personal Data Request, Orders, Warrants and Communications Data Authorisations (英国) 以及具有同等法律效力的法院命令和/或来自其它国家/地区的请求。

B. 管理和回应政府和执法机构的信息请求

Apple 会仔细审核所有法律请求，以便确保每个请求都有合法的法律依据；并会遵从合法的请求。如果 Apple 认为请求缺乏合法的法律依据或认为请求不明确、不恰当或过于宽泛，则 Apple 会反对、质疑或拒绝该请求。

考虑到相应流程和系统限制的影响，Apple 无法接受涉及 25 个以上帐户标识符的法律请求。如果执法机构提交的法律请求涉及 25 个以上帐户标识符，则 Apple 将对前 25 个请求给出回应，然后执法机构需要为其余的标识符 (如有) 重新提交新的法律请求。

C. 保存请求

美国境外的政府和执法机构在提出任何内容请求时，都必须遵守包括美国《电子通讯隐私法》(United States Electronic Communications Privacy Act，以下简称“ECPA”) 在内的适用法律，但紧急情况 (详见下文“紧急请求”中的定义) 除外。如果一方根据《法律互助条约》(Mutual Legal Assistance Treaty) 或《澄清境外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act) 下的行政协议 (以下简称“CLOUD 法案协议”) 提出请求，则符合 ECPA 的规定。要在发出 ECPA 合规请求前提交保留数据的请求，应通过电子邮件将请求发送至 lawenforcement@apple.com。

另外，根据中国的法律要求，对于将国家或地区设置为“中国”的 Apple ID，其 iCloud 服务的运营已转移至贵州，由云上贵州大数据产业发展有限公司（以下简称“GCBD”）管理。因此，自 2018 年 2 月 28 日起，与此类顾客相关的 iCloud 数据请求应通过以下电子邮件地址发送至 GCBD：china_police_requests@gzdata.com.cn。

保留请求必须注明相关的 Apple ID/帐户电子邮件地址，或是全名和电话号码，以及/或者目标 Apple 帐户的全名和邮寄地址。收到保留请求时，对于提出请求时可用的现有顾客数据，Apple 将保留一份一次性的所请求数据备份，期限为 90 天。90 天后，保留的数据将自动从存储服务器中删除。但是，如果再次提出请求，此期限可以再延长 90 天。如对同一帐户提出两次以上保留请求，则第二次请求将被视为对原始保留请求的延期请求，而不是对新数据单独提出的保留请求。

D. 紧急请求

如果相关请求涉及与紧急和严重个人生命/安全威胁、国家安全或重要基础设施/装置安全有关的情况，则 Apple 会将该请求视为紧急请求。

如果提出请求的政府部门或执法机构人员提供符合要求的确认信息，能够证明其请求涉及的紧急情况满足以上一个或多个标准，Apple 将紧急审查此类请求。

如需请求 Apple 在紧急情况下自愿披露信息，提出请求的政府或执法官员应填写“[政府部门和执法机构紧急信息请求书](#)”表单，直接通过其政府部门或执法机构官方电子邮件地址将表单发送至 exigent@apple.com，并在主题栏中注明“紧急请求”。

如果政府部门或执法机构通过填写《Emergency Government & Law Enforcement Information Request》表单请求 Apple 提供相应的顾客数据，则 Apple 可能会联系负责提交《政府部门和执法机构紧急信息请求书》的政府部门或执法机构工作人员的上级主管，请对方确认该紧急请求的合法性。提交“政府部门和执法机构紧急信息请求”的政府部门或执法机构应该在请求中提供主管的联系方式。

如果政府部门或执法机构需要就紧急问询联系 Apple，请拨打 001 408 974-2095 联系 Apple 的 Global Security Operations Center (GSOC)。该电话号码支持多种语言。

E. 帐户限制/删除请求

如果政府部门或执法机构请求 Apple 限制/删除顾客的 Apple ID，Apple 会要求提供法院命令或其他等效的国内法律文书（包括判决书或调查函），证明要限制/删除的帐户存在非法使用的情况。

Apple 会仔细审查政府和执法机构的所有请求，以确保每个请求都具有有效的法律依据。如果 Apple 确定请求无有效的法律依据，或者如果法院命令未证明要限制/删除的帐户存在非法使用的情况，Apple 将拒绝/质疑该请求。

如果 Apple 从政府部门或执法机构收到符合要求的法院命令或其他等效的国内法律文书 (通常为判决书或调查函)，证明要限制/删除的帐户存在非法使用的情况，Apple 将遵从法院命令，采取必要措施来限制/删除该帐户；同时将相关过程告知发出请求的机构。

F. 客户通知

为了回应政府部门或执法机构提出的合法有效的请求而查询顾客的 Apple 帐户信息时，Apple 会通知这些顾客，除非存在以下情况：合法有效的请求、Apple 收到的法院命令以及适用法律明确禁止提供通知；或者 Apple 单方面认为提供通知会给身份明确的个人造成伤害或死亡的风险、案件涉及儿童侵害，或者通知不适用于案件的基本事实。

90 天后，Apple 会就紧急信息披露请求提供延迟通知，除非存在以下情况：法院命令或适用法律明确禁止提供通知；或者 Apple 单方面认为提供通知可能会给身份明确的个人或群体造成伤害或死亡的风险，或者案件涉及儿童侵害。法院命令中规定的保密期过后，Apple 将提供延期通知，除非 Apple 单方面有理由认为提供通知可能会给身份明确的个人或群体造成伤害或死亡的风险，或者案件涉及儿童侵害，或者通知不适用于案件的基本事实。

如果 Apple 收到的法院命令 (通常为判决书或调查函) 证明要求限制/删除的账户存在非法使用或违反 Apple 服务条款的情况，则 Apple 为了回应而限制/删除用户的账户时会通知用户；除非存在以下情况：法律文书本身、Apple 收到的法院命令、适用法律明确禁止提供通知；案件涉及儿童侵害；Apple 单方面有理由认为提供通知会给身份明确的个人或群体带来伤害或死亡的风险；通知不适用于案件的基本事实；Apple 有理由认为提供通知可能会妨碍司法公正或破坏司法管理。

III. Apple 可以提供的信息

本部分涵盖了在发布本指南时 Apple 可以提供的常见信息类型。

A. 设备注册

对于早于 iOS 8 和 Mac OS Sierra 10.12 的操作系统，顾客在注册 Apple 设备时，会向 Apple 提供基本注册或顾客信息，包括姓名、地址、电子邮件地址和电话号码。Apple 不会验证这些信息，因此这些信息可能不准确或无法反映设备的所有者。对于运行 iOS 8 及更高版本的设备以及运行 Mac OS Sierra 10.12 及更高版本的 Mac，在顾客将设备关联到 iCloud Apple ID 时，Apple 会收到相关注册信息。这些信息可能不准确或无法反映设备的所有者。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取注册信息 (如有)。

请注意，Apple 设备序列号不包含字母“O”或“I”，而是在序列号中使用数字 0 (零) 和 1 (一)。如果关于序列号的请求中包含字母“O”或“I”，则该请求不会收到任何结果。

B. 顾客服务记录

可以从 Apple 获取有关顾客就设备或服务与 Apple 顾客服务部门进行联系的信息。这些信息可能包括就特定 Apple 设备或服务与顾客进行的支持互动记录。此外，我们可能还可以提供有关设备、保修和维修的信息。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取这些信息 (如有)。

C. Apple 媒体服务

App Store、Apple Music、Apple TV app、Apple 播客和 Apple Books (以下统称“Apple 媒体服务”) 是指顾客用于整理和使用 app、播放数字音乐和视频以及播放流媒体内容的软件应用程序。Apple 媒体服务还为顾客提供可下载到电脑和 iOS 设备的内容。顾客在开设 Apple 帐户时，会提供基本顾客信息，例如姓名、邮寄地址、电子邮件地址和电话号码。此外，系统可能还会显示关于 Apple 媒体服务、购买/下载交易和连接信息、更新/下载连接信息。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取 Apple 媒体服务顾客信息以及包含 IP 地址的连接日志 (如有)。

关于 Apple 媒体服务数据的请求必须提供 Apple 设备标识符 (序列号、IMEI、MEID 或 GUID) 或相关的 Apple ID/帐户电子邮件地址。如果无法提供 Apple ID/帐户电子邮件地址，则需要采用全名加上电话号码和/或全名加上邮寄地址的形式向 Apple 提供 Apple 媒体服务顾客信息，以便识别目标 Apple 媒体服务顾客帐户。政府或执法机构人员还可以提供与 Apple 媒体服务购买交易相关的有效 Apple 媒体服务订单号或完整的借记卡或信用卡卡号，也可以组合提供顾客姓名和上述数据。但如果仅提供顾客姓名，则无法获取信息。

请注意：如果你的法律请求包含完整的信用卡/借记卡数据，出于数据安全目的，信用卡/借记卡数据应以密码保护/加密的文档/文件形式发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。

D. Apple Store 零售店交易

销售点交易是指在 Apple Store 零售店完成的现金、信用卡/借记卡或礼品卡交易。针对销售点记录的请求必须包含所使用的完整信用卡/借记卡卡号，还可以包含其他信息，例如交易日期和时间、金额和购买的商品。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取与特定购买交易相关的银行卡类型、购买者姓名、电子邮件地址、交易日期/时间、交易金额和零售店相关的信息 (如有)。

对收据副本的请求必须包括与购买相关的零售交易号码，如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取相关信息 (如有)。

请注意：如果你的法律请求包含完整的信用卡/借记卡数据，出于数据安全目的，信用卡/借记卡数据应以密码保护/加密的文档/文件形式发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。

E. Apple Store 在线商店购买交易

Apple 会保留有关 Apple Store 在线商店购买交易的信息，这些信息可能包括购买者姓名、送货地址、电话号码、电子邮件地址、购买的产品、购买数量和购买时的 IP 地址。针对有关 Apple Store 在线商店订单的信息提出的请求必须包含完整的信用卡/借记卡卡号，或者所购商品的订单号或序列号。也可以

组合提供顾客姓名和上述数据，但如果仅提供顾客姓名，则无法获取信息。此外，针对有关 Apple Store 在线商店订单信息的请求可以包含相关的 Apple ID/帐户电子邮件地址。如果无法提供 Apple ID/帐户电子邮件地址，则根据 Apple 的要求，需要采用全名加上电话号码和/或全名加上邮寄地址的形式，以便识别目标 Apple 帐户。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取 Apple Store 在线商店购买交易的信息 (如有)。

请注意：如果你的法律请求包含完整的信用卡/借记卡数据，出于数据安全目的，信用卡/借记卡数据应以密码保护/加密的文档/文件形式发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。

F. 礼品卡

Apple Store 礼品卡以及 App Store 和 iTunes Store 礼品卡均具有序列号和 PIN 码 (又称为兑换 PIN 码)。Apple Store 礼品卡以及 App Store 和 iTunes Store 礼品卡均具有多种序列号格式，具体取决于设计和/或发行日期等因素。无论用户拥有哪种类型的礼品卡，都可以通过兑换 PIN 码使用礼品卡上的余额。Apple 搜索礼品卡的相关信息时，礼品卡 PIN 码是最可靠的参数。如果请求方提出在所在国家/地区合法有效的正当请求，则 Apple 可以提供 Apple Store 礼品卡以及 App Store 和 iTunes Store 礼品卡的相关信息。如果法律请求包含 5 个或更多礼品卡 PIN 码，则 Apple 要求以可编辑的电子格式提交这些礼品卡 PIN 码。

i. Apple Store 礼品卡

Apple Store 礼品卡可用于在 Apple Store 在线商店或 Apple Store 零售店中进行购买。Apple Store 礼品卡上的 PIN 码以字母“Y”开头。在某些情况下，发行时间较早的 Apple Store 礼品卡可能会采用 8 位 PIN 码格式。可以提供的记录可能包括礼品卡购买者信息 (如果是通过 Apple 而不是通过第三方商家购买)、相关购买交易和已购买的物品。在某些情况下，Apple 可能会取消或暂停接受 Apple Store 礼品卡，具体取决于卡片状态。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取 Apple Store 礼品卡信息 (如有)。

请注意：如果你的法律请求包含完整的 Apple Store 礼品卡数据，出于数据安全目的，Apple Store 礼品卡数据应以密码保护/加密的文档/文件形式发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。

ii. App Store 和 iTunes 礼品卡

App Store 和 iTunes 礼品卡可在 Apple Music、App Store、Apple Books 和 Mac App Store 中使用。App Store 和 iTunes 礼品卡上的 PIN 码以字母“X”开头。有了 PIN 码，Apple 可以确定 App Store 和 iTunes 礼品卡是否已经激活 (通过零售店销售点购买) 或兑换 (添加至 Apple 帐户的商店余额)。

App Store 和 iTunes 礼品卡激活后，可以提供的记录可能包括商店名称、位置、日期和时间。App Store 和 iTunes 礼品卡兑换完毕后，可以提供的记录可能包括相关 Apple 帐户的顾客信息、激活和/或兑换的日期和时间以及兑换时的 IP 地址。在某些情况下，Apple 可能会禁用 App Store 和 iTunes 礼品卡，具体取决于卡片状态。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取 App Store 和 iTunes 礼品卡 (如有)。

请注意：如果你的法律请求包含完整的 App Store 和 iTunes 礼品卡数据，出于数据安全目的，App Store 和 iTunes 礼品卡数据应以密码保护/加密的文档/文件形式发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。

G. Apple Pay

在零售店店面 (例如：通过 NFC/无接触式通信)、app 内或在线销售的完成的 Apple Pay 交易会在顾客的设备上以安全方式进行身份信息验证，交易数据会以加密形式发送给商家或商家的付款处理方。虽然交易安全信息是由 Apple 服务器验证的，但 Apple 不负责处理付款，也不会存储此类交易数据或使用 Apple Pay 所进行购买的相关完整信用卡/借记卡号。上述信息可通过相关发卡行、支付网络或商家获取。

如需进一步了解哪些国家和地区支持 Apple Pay，请访问 <https://support.apple.com/zh-cn/HT207957>。

对于在 Apple Store 零售店完成的购买，如需向 Apple 请求交易数据，则需要提供设备主帐户号 (DPAN ID)，这是一种经过哈希处理的标识符，通常为 64 位。可通过发卡行获取。要获取与 Apple 交易相关的 DPAN ID，请联系发卡行。Apple 可使用相关 DPAN ID 信息在合理范围内进行搜索，通过其销售点系统找到相应信息。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取这些信息 (如有)。

Apple 可提供以下 Apple Pay 信息：顾客添加到 Apple Pay 的信用卡/借记卡类型，以及顾客信息。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取这些信息 (如有)。要向 Apple 请求此类信息，则需要提供设备标识符 (Apple 序列号、SEID、IMEI 或 MEID)；或是 Apple ID/帐户电子邮件地址。

请注意：如果你的法律请求包含完整的 DPAN ID，出于数据安全目的，此类数据应以密码保护/加密的文档/文件形式发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。

H. iCloud

iCloud 是 Apple 的云服务，可帮助顾客通过他们的各种设备访问自己的音乐、照片、文稿等内容。顾客还可以通过 iCloud 将其 iOS 设备备份到 iCloud。借助 iCloud 服务，顾客可以设置 iCloud.com 电子邮件帐户。iCloud 电子邮件域名可以是 @icloud.com、@me.com 和 @mac.com。Apple 存储的所有 iCloud 内容数据都会在服务器本地经过加密。如果使用第三方提供商存储数据，Apple 不会向其提供密钥。Apple 将加密密钥保存在其美国数据中心。

iCloud 面向顾客提供的服务。关于 iCloud 数据的请求必须包含相关的 Apple ID/帐户电子邮件地址。如果无法提供 Apple ID/帐户电子邮件地址，则根据 Apple 的要求，需要采用全名加上电话号码和/或全名加上邮寄地址的形式，以便识别目标 Apple 帐户。如果请求方仅提供电话号码，或是仅提供 Apple ID/帐户电子邮件地址，则可以提供与这些要素相关的已验证帐户的信息。

iCloud 可以提供以下信息：

i. 顾客信息

顾客设置 iCloud 帐户时，可能会向 Apple 提供基本顾客信息，例如姓名、邮寄地址、电子邮件地址和电话号码。此外，我们可能还会提供有关 iCloud 功能连接的信息。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取 iCloud 顾客信息以及包含 IP 地址的连接日志(如有)。连接日志最多保留 25 天。

ii. 邮件日志

邮件日志包括入站和出站通信的记录，例如时间、日期、发件人电子邮件地址和收件人电子邮件地址。iCloud 邮件日志最多保留 25 天；如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取邮件日志(如有)。

iii. 电子邮件内容和其他 iCloud 内容。我的照片流、iCloud 照片图库、iCloud 云盘、通讯录、日历、书签、Safari 浏览器浏览历史记录、地图搜索历史记录、信息、iOS 设备备份

顾客的帐户保持活跃状态时，iCloud 会存储顾客选择保留在帐户中的服务内容。内容一旦从 Apple 的服务器中清除，Apple 就不会保留已删除的内容。iCloud 内容可能包括电子邮件、存储的照片、文档、通讯录、日历、书签、Safari 浏览器浏览历史记录、地图搜索历史记录、消息和 iOS 设备备份。iOS 设备备份可包括相机胶卷、设备设置、app 数据、iMessage 信息、商务聊天、SMS、MMS 消息和语言信箱中的照片和视频。Apple 存储的所有 iCloud 内容数据都会在服务器本地经过加密。如果使用第三方提供商存储数据，Apple 不会向其提供密钥。Apple 将加密密钥保存在其美国数据中心。

美国境外的政府和执法机构在提出任何内容请求时，都必须遵守包括美国《电子通讯隐私法》(United States Electronic Communications Privacy Act，以下简称“ECPA”)在内的适用法律，但紧急情况（详见上文“紧急请求”中的定义）除外。如果一方根据《法律互助条约》(Mutual Legal Assistance Treaty) 或《澄清境外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act) 下的行政协议（以下简称“CLOUD 法案协议”）提出请求，则符合 ECPA 的规定。Apple 仅在回应此类合法有效的流程时才会提供顾客内容，因为该内容存储在顾客的帐户中。

另外，根据中国的法律要求，对于将国家或地区设置为“中国”的 Apple ID，其 iCloud 服务的运营已转移至贵州，由云上贵州大数据产业发展有限公司（以下简称“GCBD”）管理。因此，自

2018 年 2 月 28 日起，与此类顾客相关的 iCloud 数据请求应通过以下电子邮件地址发送至 GCBD：china_police_requests@gzdata.com.cn。

I. “查找”

“查找”是一项由用户启用的功能，通过该功能，iCloud 顾客能够找到他/她丢失或遗忘的 iPhone、iPad、iPod touch、Apple Watch、AirPods 或 Mac，并且/或者采取某些措施，包括将该设备设置为丢失模式，或锁定或擦除该设备。有关这项服务的更多信息，请访问 <https://www.apple.com.cn/icloud/find-my/>。

如果已经丢失设备的顾客想要使用“查找”功能，则必须在相应设备丢失前就已经启用此功能。“查找”功能无法在设备丢失后激活，无法远程激活，也无法根据政府部门或执法机构提出的请求激活。设备位置服务信息存储在各个设备上，Apple 无法从任何特定设备检索此信息。通过“查找”功能找到的设备的位置服务信息是面向顾客的，Apple 未存储通过该服务发送的地图或提醒内容。如果顾客的 iOS 设备丢失或被盗，可访问以下支持链接了解相关信息以及可以采取的措施：<http://support.apple.com/zh-cn/HT201472>。

“查找”连接日志的有效期大约为 25 天；如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取“查找”连接日志（如有）。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取“查找”交易活动数据（如有），相关数据包括远程锁定或抹掉设备的请求。

J. 从密码锁定的 iOS 设备中提取数据

对于运行 iOS 8.0 及更高版本的所有设备，Apple 无法执行 iOS 设备数据提取，因为执法机构需要查询的数据通常都是加密数据，而 Apple 不持有加密密钥。所有 iPhone 6 及更新设备机型在制造出厂时都运行 iOS 8.0 或更高版本的 iOS。

对于运行 iOS 4 至 iOS 7 的设备，Apple 可以根据《加利福尼亚的电子通讯隐私法》(CalECPA，《加州刑法典》第 1546-1546.4 条) 执行 iOS 数据提取，具体取决于设备状态。为了让 Apple 对符合这些标准的设备执行 iOS 数据提取，执法机构应该获取搜查令，该搜查令应该基于 CalECPA 中说明的可能原因而发出。除了 CalECPA 以外，Apple 尚未认可任何其他已知法律机构作为执法调查的第三方来要求 Apple 提取数据。

K. 其他可提供的设备信息

MAC 地址：媒体访问控制地址 (MAC 地址) 是分配给网络接口用于在实体网络段上进行通信的唯一标识符。任何带网络接口，例如蓝牙、以太网、Wi-Fi 或 FireWire 的 Apple 产品，都有一个或多个 MAC 地址。如果请求方提出在所在国家/地区合法有效的正当请求，并向 Apple 提供序列号 (对于 iOS 设备，则提供 IMEI、MEID 或 UDID)，则可获取相应的 MAC 地址信息 (如有)。

L. Apple Store 零售店闭路电视数据请求

闭路电视数据可能因具体零售店而异。通常，Apple Store 零售店的闭路电视数据最多保留 30 天。在很多司法管辖区，考虑到当地法律，该期限短至二十四 (24) 小时。超出该时间范围后，数据可能已删除。如果请求仅与闭路电视数据有关，可发送至 lawenforcement@apple.com。政府部门或执法机构应该提供有关所请求数据的具体日期、时间和相关交易信息。

M. Game Center

Game Center 是 Apple 的社交游戏网络。可提供有关顾客或设备的 Game Center 连接信息。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取包含 IP 地址的连接日志和交易记录 (如有)。

N. iOS 设备激活

当顾客通过蜂窝网络服务提供商激活 iOS 设备，或是升级软件时，服务提供商或设备可向 Apple 提供某些信息，具体取决于相应事件。可提供事件的 IP 地址、ICCID 编号和其它设备标识符。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取这些信息 (如有)。

双卡：对于支持双卡的设备，如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取 nano SIM 和/或 eSIM 的运营商信息 (如有)。eSIM 是一种数字 SIM 卡，让顾客可以通过运营商激活蜂窝网络套餐，而无需使用实体 nano-SIM 卡。更多相关信息，请访问 <http://support.apple.com/zh-cn/HT209044>。在中国大陆、中国香港和中国澳门，iPhone 11、iPhone 11 Pro、iPhone 11 Pro Max、iPhone XS Max 和 iPhone XR 上的双卡功能需使用两张 nano-SIM 卡实现。

O. 连接日志

顾客或设备连接到 Apple 服务的连接活动，例如 Apple Music、Apple TV app、Apple 播客、Apple Books、iCloud、我的 Apple ID 和 Apple Discussions (如有) 均可通过 Apple 获取。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取包含 IP 地址的连接日志 (如有)。

P. “我的 Apple ID”和 iForgot 日志

顾客的“我的 Apple ID”和 iForgot 日志可通过 Apple 获取。“我的 Apple ID”和 iForgot 日志可能包括有关密码重设操作的信息。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取包含 IP 地址的连接日志 (如有)。

Q. FaceTime 通话

FaceTime 通信是经过端到端加密的，Apple 无法在设备之间传输 FaceTime 通话数据时解密这些数据。Apple 无法拦截 FaceTime 通信。在用户发起 FaceTime 通话邀请时，Apple 会生成 FaceTime 通话邀请日志。这些日志并不表示顾客之间实际发生了任何通信。FaceTime 通话邀请日志最多保留 25

天。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取 FaceTime 通话邀请日志 (如有)。

R. iMessage 信息

iMessage 信息通信是经过端到端加密的，Apple 无法在设备之间传输 iMessage 信息数据时解密这些数据。Apple 无法拦截 iMessage 信息通信，而且 Apple 没有任何 iMessage 信息通信日志。Apple 确实有 iMessage 信息功能查询日志。这些日志表明设备应用程序 (可能是消息、通讯录、电话或其他设备应用程序) 已经发起查询，并将其路由到 Apple 的服务器以获取查询句柄 (可能是电话号码、电子邮件地址或 Apple ID)，从而确定查询句柄是否支持 iMessage 信息。iMessage 信息功能查询日志不表示顾客之间实际发生了任何通信。Apple 无法根据 iMessage 信息功能查询日志来确定是否发生了任何实际的 iMessage 信息通信。Apple 也无法识别发起该查询的实际应用程序。iMessage 信息功能查询日志不确认是否实际尝试了 iMessage 事件。iMessage 信息功能查询日志最多保留 25 天。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取 iMessage 信息功能查询日志 (如有)。

S. Apple TV app

顾客可使用 Apple TV app 浏览、购买、订阅和播放 Apple TV+、Apple TV Channel、第三方 app 和服务提供的电视节目和电影。可提供购买和下载历史记录。

关于 Apple TV app 顾客数据的请求必须提供 Apple 设备标识符 (序列号、IMEI、MEID 或 GUID) 或相关的 Apple ID/帐户电子邮件地址。如果无法提供 Apple ID/帐户电子邮件地址，则需要采用全名加上电话号码和/或全名加上邮寄地址的形式向 Apple 提供顾客信息，以便识别目标顾客帐户。政府部门或执法机构还可以提供有效的 Apple 订单号或与 Apple TV app 购买内容相关的完整信用卡/借记卡号。也可以组合提供顾客姓名和上述数据，但如果仅提供顾客姓名，则无法获取信息。

请注意：如果你的法律请求包含完整的信用卡/借记卡数据，出于数据安全目的，此类数据应以密码保护/加密的文档/文件形式发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。

T.通过 Apple 登录

“通过 Apple 登录”是一种更私密的方式，顾客可通过这种方式使用自己现有的 Apple ID 登录第三方 app 和网站。参与该计划的 app 或网站上会显示“通过 Apple 登录”按钮，点击该按钮后，顾客可设置帐户并使用自己的 Apple ID 登录。顾客无需使用社交媒体帐户，也不用填写表单并选择另一个新密码，只需轻点“通过 Apple 登录”按钮，核对个人信息，即可使用面容 ID、触控 ID 或自己的设备密码快速安全地登录。更多相关信息，请访问 <http://support.apple.com/zh-cn/HT210318>。

“隐藏邮件地址”是“通过 Apple 登录”的一项功能，使用 Apple 的私密电子邮件中转服务创建和共享唯一的随机电子邮件地址，可将电子邮件转发到顾客的个人电子邮件地址。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取基本顾客信息。

IV. 常见问题解答

问：我是否可以通过电子邮件向 **Apple** 发送有关执法机构信息请求的问题？

答：是，有关政府法律程序的问题或咨询可通过电子邮件发送到 lawenforcement@apple.com。

问：设备是否必须通过 **Apple** 注册以后才可以正常使用？

答：不，设备无需为了使其运行或使用而向 **Apple** 注册。

问：**Apple** 可以提供我当前锁定的 iOS 设备的密码吗？

答：不可以，**Apple** 无权访问顾客密码。

问：你可以帮我丢失或被盗的设备退还给失主吗？

答：在这些情况下，请联系 lawenforcement@apple.com。请提供设备的序列号或 IMEI 号以及任何其他相关信息。如果顾客信息可以提供，我们将与顾客联系并建议他/她联系执法部门以恢复设备。但如果无法通过提供的信息确定顾客，你可以按照相关说明提交有效的法律请求。

问：**Apple** 是否保留丢失或被盗设备列表？

答：否，**Apple** 不保留丢失或被盗设备列表。

问：如果执法机构结束了调查/刑事案件，应该如何处理 **Apple** 提供的回应信息？

答：在相关调查、刑事案件和所有申诉完全结束以后，提供给政府部门或执法机构的包含个人身份信息的信息和数据 (包括所有副本) 应销毁。

问：在收到与顾客相关的执法机构信息请求时，**Apple** 是否会通知这些顾客？

答：是，**Apple** 的通知政策适用于执法机构、政府和私人机构提出的帐户请求。**Apple** 将会通知顾客和帐户持有人，除非收到保密命令或适用法律禁止提供通知，或者 **Apple** 单方面有理由认为此类通知会立即给公众带来严重伤害或死亡的风险、案件涉及儿童侵害问题或者通知不适用于案件的基本事实。