法律程序指南

美国境外的政府和执法机构

本指南供美国境外的政府和执法机构在从 Apple 的相关实体 (在相关地区或国家提供服务) 寻求有关 Apple 设备、产品和服务的用户信息时使用。Apple 在必要时将更新这些指南。

在本指南中，Apple 须指在特定地区或国家对客户/用户信息负责任的相关实体。Apple 作为一家全球性的公司，在不同的司法管辖区拥有多个法律实体，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终端信息将由各个国家/地区的各个 Apple 零售店实体控制。根据具体管辖区内各项服务的相关条款，Apple Store 在线商店和 iTunes 相关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 (澳大利亚、加拿大、爱尔兰和日本) 的法律实体负责其所在地区内与 Apple 服务相关用户数据。

所有其它关于 Apple 客户/用户信息的请求，包括关于信息披露的客户/用户问题，请参阅 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 遵守适用于控制数据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 (ECPA)》在内的适用法律，但紧急情况 (见下面“紧急请求”中的定义) 除外。根据与美国签署的双边司法互助条约或协议而提出的请求符合 ECPA。

根据中国的法律要求，在其国家或地区设置的与中国 Apple ID 相关的 iCloud 服务的运营已通过云上贵州大数据产业发展有限公司 (云上贵州) 转移至贵州。因此，自 2018 年 2 月 28 日生效起，与此类客户相关的 iCloud 数据请求应通过以下电子邮件地址发送至云上贵州：china_police_requests@gzdata.com.cn.

对于私人机构请求，Apple 遵守与控制用户数据并按法律要求提供数据的当地实体相关的法律。

对于接收、跟踪、处理和回应来自政府、执法机构和私人机构的合法法律请求，Apple 有从收到这些请求到 做出回应的集中流程。我们的法律部门中有训练有素的团队，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

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、Apple TV、Apple Watch、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 iTunes Store、App Store、iBookstore 和 Mac App Store 销售和提供数字内容和应用程序。对于特定服务产品，Apple 根据 Apple 的隐私政策和适用的服务条款/条款和条件保留用户信息。Apple 致力于维护 Apple 产品和服务的用户 (下称“Apple 用户”) 的隐私。因此，如果没有有效的法律程序，Apple 将不会提供 Apple 用户相关信息。

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。下列准则并非为了提供法律建议。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。

如果还有其他问题，请联系 lawenforcement@apple.com。

上述邮箱仅限政府和执法机构人员使用。如果选择向该地址发送电子邮件，发件人必须是政府或执法机构的有效官方电子邮件地址。

Apple 收到的大多数执法机构请求都是寻求特定 Apple 设备或客户相关信息，以及 Apple 可能向该客户提供的具体服务。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 设备或客户信息。Apple 会保留在下面特定的“可提供信息”部分中所列的数据。所有其它数据将保留一段时间，以满足我们的隐私政策中所述的目的。政府和执法机构在提出请求时应该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、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 (ECPA) 》在内的适用法律，但紧急情况 (见下面“紧急请求”中的定义) 除外。根据与美国签署的双边司法互助条约或协议而提出的请求符合 ECPA。

本指南中的任何内容都不是为了构成针对 Apple 的任何具有法律效力的权利，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 接受政府和执法机构通过电子邮件送达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或执法机构的官方电子邮件地址发出的。美国境外的政府和执法机构人员在向 Apple 提交信息请求时，应填写政府和执法机构信息请求模板，然后从政府或执法机构的官方电子邮件地址将该模板直接提交到此邮箱：lawenforcement@apple.com。

上述邮箱仅限政府和执法机构人员使用。如果选择向该地址发送电子邮件，发件人必须是政府或执法机构的有效官方电子邮件地址。如果请求包含五个或更多标识符，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进行发送。通常在进行与设备、账户或财务交易相关信息的搜索时需要用到此类标识符。

如果执法机构提出的信息请求在其所在国家/地区的国内法律中具有确切的法律依据，并且涉及真正的犯罪预防、侦查或调查，则 Apple 认为这样的信息请求合法有效。Apple 认为合法有效并接受的国际请求的例子包括：生产订单 (澳大利亚、加拿大)、法庭命令 (新西兰)、请求或司法调查委员会函 (法国)、数据请求 (西班牙)、司法秩序 (巴西)、信息请求 (德国)、Obligation de dépôt (瑞士)、要求披露个人信息 (日本)、个人数据申请 (英国) 以及相应的法院命令和/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请求

Apple 会仔细审核来自政府、执法机构和私人机构的所有请求，以确保每个请求都具有有效的法律依据；并按照合法有效的请求提供信息。如果 Apple 确定请求缺乏有效的法律依据或认为请求不明确、不恰当或过于宽泛，则 Apple 会质疑或拒绝该请求。

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 (ECPA)》在内的适用法律，但紧急情况 (见下面“紧急请求”中的定义) 除外。根据与美国签署的双边司法互助条约或协议而提出的请求符合 ECPA。要在即将发出的 ECPA 合规请求前提交保留数据的请求，应通过电子邮件发送到 Apple Inc. 的邮箱：lawenforcement@apple.com。

根据中国的法律要求，在其国家或地区设置的与中国 Apple ID 相关的 iCloud 服务的操作已通过云上贵州大数据产业发展有限公司 (云上贵州) 转移 至贵州。因此，自 2018 年 2 月 28 日生效起，与此类客户相关的iCloud数据请求应通过以下电子邮件地址发送至云上贵州：china_police_requests@gzdata.com.cn。

保留请求必须包括相关的 Apple ID/账户电子邮件地址或全名**和**电话号码，以及 (或) 目标 Apple 账户的全名**和**实际地址。当 Apple Inc. 收到保留请求时，将对所请求的现有用户数据进行一次性收集并保留备份，期限为从提交请求开始 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。针对同一账户的两次以上的保留请求将被视为针对原保留数据的延期请求，但 Apple Inc. 在回应此类请求时，不会保留新数据。

D. 紧急请求

当一项请求涉及以下内容造成迫在眉睫的严重威胁时，Apple 认为该请求属于紧急请求：

1) 个人的生命/安全；
2) 国家/地区的安全；

3) 关键基础设施/装置的安全。

如果提出请求的政府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。

要向 Apple 提出紧急请求，发出请求的政府或执法官员应填写 《紧急政府和执法机构信息请求表》，并直接从其官方政府或执法机构的电子邮件地址发送到邮箱：exigent@apple.com，并在主题栏中加上“紧急请求”一词。

Apple 在提供客户数据以回应“政府和执法机构紧急信息请求”时，会联系提交“政府和执法机构紧急信息请求”的政府或执法机构的指定主管，并要求该主管向 Apple 确认该紧急请求的合法性。提交“政府和执法机构紧急信息请求”
的政府或执法机构应该在请求中提供主管的联系方式。

如果政府或执法机构需要在非工作时间 (美国太平洋时间上午 8:00 以前或下午 5:00 以后) 联系 Apple 进行紧急咨询，请拨打 001 408 974-2095 联系 Apple 全球安全运营中心 (Global Security Operations Center, GSOC)。该电话号码提供多种语言的支持。

E. 账户限制/删除请求

如果政府或执法机构请求 Apple 限制/删除客户的 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/删除的账户存在非法使用的情况。在收到非官方/无效的请求时，Apple 不会限制/删除客户的账户。

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/删除的账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 (包括判决书或调查函)，证明要限制/删除的账户存在非法使用的情况，Apple 将遵从法院命令采取必要措施限制/删除该账户；同时将相关过程通知发出请求的机构。

F. 用户通知

为了回应政府或执法机构提出的合法有效的请求而查询客户/用户的 Apple 账户信息时，Apple 会通知这些客户/用户，除非合法有效的请求、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，通知不适用于案件的基本事实，Apple 合理地认为提供通知可能会妨碍司法公正或破坏司法管理。

90 天后，Apple 将就紧急信息披露请求向客户提供延迟通知，除非法院命令或适用法律明确禁止提供通知；或者 Apple 单方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，或案件涉及

儿童侵害。Apple将在法院命令中指定的保密期限到期后提供延迟通知，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，案件涉及儿童侵害、通知不适用于案件的基本事实，Apple 合理地认为提供通知可能会妨碍司法公正或破坏司法管理。

如果 Apple 收到的法院命令 (包括判决书或调查函) 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：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造成伤害或死亡的风险；通知不适用于案件的基本事实；Apple 合理地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，客户在注册 Apple 设备时，会向 Apple 提供基本注册或客户信息，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，在客户将设备关联到 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. 客户服务记录

可以从 Apple 获取有关客户就设备或服务与 Apple 客户服务部门进行联系的信息。这些信息可能包括就特定 Apple 设备或服务与客户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. iTunes

iTunes 是一款免费软件应用程序，客户可以使用 iTunes 在其电脑上整理和播放数字音乐和视频。iTunes 还是一个商店，提供可供客户下载到自己的电脑和 iOS 设备上的内容。客户在开设 iTunes 账户时，会提供基本订阅用户信息，例如姓名、实际地址、电子邮件地址和电话号码。此外，我们还可能提供与 iTunes 购买交易/下载交易和连接、更新/重新下载连接以及 iTunes Match 连接相关的信息。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 iTunes 订阅用户信息和带有 IP 地址的连接日志 (如有)。

关于 iTunes 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/账户电子邮件地址。如果 Apple ID/账户电子邮件地址不明，则有必要采用全名**搭配**电话号码和/或全名**搭配**实际地址的形式向 Apple 提供 iTunes 订阅用户信息，以便识别目标 iTunes 订阅用户账户。政府或执法机构人员还可以提供与 iTunes 购买交易相关的有效 iTunes 订单号或完整的借记卡或信用卡卡号。同时也可提供客户姓名和这些参数，但仅提供客户姓名不足以获取信息。

请注意：如果您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/文件形式传输到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件传输。

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联的银行卡类型、购买者姓名、电子邮件地址、交易日期/时间、交易金额和商店位置相关的信息 (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，可以通过向请求者所在国家发出适当、合法、有效的请求来获取 (如有)。

请注意：如果您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/文件形式传输到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件传输。

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、参考号或序列号。可以同时提供客户姓名和这些参数，但仅提供客户姓名不足以获取信息。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/账户电子邮件地址。如果 Apple ID/账户电子邮件地址不明，则 Apple 需要的订阅用户信息应采用全名**搭配**电话号码和/或全名**搭配**实际地址的形式，以便识别目标 Apple 账户。如果请求方提出在所在国家/地区合法有效的请求，则可以获取 Apple Store 在线商店购买交易的信息 (如有)。

请注意：如果您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/文件形式传输到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件传输。

F. 礼品卡

Apple Store 礼品卡和 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/或发布日期等变量。任一礼品卡类型的持有人均可以通过兑换 PIN 码使用礼品卡上的资金。礼品卡 PIN 码是 Apple 用于搜索礼品卡相关信息的最可靠参数。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，较旧的 Apple Store 礼品卡可能包含 8 位数的 PIN 码格式。可用记录可能包括礼品卡购买者信息 (如果从 Apple 购买，而不是从第三方商家购买)、相关的购买交易以及购买的商品。在某些情况下，Apple 可能会取消或暂停 Apple Store 礼品卡，具体取决于特定礼品卡的状态。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：如果您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/文件形式传输到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件传输。

ii. iTunes Store 礼品卡

iTunes Store 礼品卡可在 iTunes Store、App Store、iBooks Store 和 Mac App Store 使用。iTunes Store 礼品卡上的 PIN 码以字母“X”开头。有了 PIN 码，Apple 可以确定 iTunes Store 礼品卡是否已经激活 (在零售店销售点进行了购买) 或兑换 (添加至 iTunes 账户的商店信用余额)。

iTunes Store 礼品卡激活后，可用记录可能包括商店名称、位置、日期和时间。iTunes Store 礼品卡兑换后，可用记录可能包括相关 iTune 账户的订阅者信息、激活和/或兑换的日期和时间以及兑换 IP 地址。在某些情况下，Apple 可能会停用 iTunes Store 礼品卡，具体取决于特定礼品卡的状态。iTunes Store 礼品卡信息 (如有) 可能会通过适用于申请者所在国家/地区的合法有效请求获取。

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

G. iCloud

iCloud 是 Apple 的云服务，允许用户从其所有设备上访问音乐、照片、文档等等。订阅用户还可以通过 iCloud 将其 iOS 设备备份到 iCloud。借助 iCloud 服务，订阅用户可以设置 iCloud.com 电子邮件账户。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 是基于订阅用户的服务。关于 iCloud 数据的请求必须包含相关的 Apple ID/账户电子邮件地址。如果 Apple ID/账户电子邮件地址不明，则 Apple 需要的订阅用户信息应采用全名搭配电话号码和/或全名搭配实际地址的格式，以便识别目标 Apple 账户。

iCloud 可能可以提供以下信息：

i. 订阅信息

用户设置 iCloud 账户时，可能会向 Apple 提供基本订阅用户信息，例如姓名、实际地址、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 订阅用户信息和带 IP 地址的连接日志 (如有)。连接日志最多保留 30 天。

ii. 邮件日志

iCloud 邮件日志包括传入和传出通信的记录，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 30 天；如果请求方提出所在国家/地区合法有效的正当请求，则可以获取该日志 (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、消息、iOS 设备备份

在订阅用户的账户保持活跃状态时，iCloud 会存储订阅用户选择保留在账户中的服务内容。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 (ECPA) 》在内的适用法律，但紧急情况 (见下面“紧急请求”中的定义) 除外。根据与美国签署的

双边司法互助条约或协议而提出的请求符合 ECPA。Apple Inc. 仅在回应此类合法有效的文书时才会提供订阅用户内容，因为该内容存在于订阅用户的账户中。

H. 查找我的 iPhone

“查找我的 iPhone”是一项用户启用的功能，通过该功能，iCloud 订阅用户能够找到他/她丢失或遗忘的 iPhone、iPad、iPod touch、Apple Watch 或 Mac 和/或采取某些措施，包括将该设备设置为丢失模式，或锁定或擦除该设备。有关此服务的更多信息，请参阅 http://www.apple.com/cn/icloud/find-my-iphone.html。

如果已经丢失设备的用户想要使用“查找我的 iPhone”功能，则必须在特定设备丢失前就已经启用了此功能。“查找我的 iPhone”功能无法在设备丢失后激活，无法远程激活，也无法根据政府或执法部门提出的请求激活。设备位置服务信息存储在每台独立的设备上，Apple 无法从任何特定设备检索此信息。通过“查找我的 iPhone”功能找到的设备的位置服务信息是面向用户的，Apple 不会获得该服务发送的地图或警报。如果 iOS 设备丢失或被盗，以下支持链接提供了所需的信息和用户可以采取的步骤：http://support.apple.com/zh-cn/HT201472。

“查找我的 iPhone”连接日志的有效期大约为 30 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“查找我的 iPhone”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“查找我的 iPhone”请求远程锁定或擦除设备的事务性活动信息 (如有)。

I. 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，对于任何其他要求 Apple 作为执法调查的第三方提取数据的已知法律机构，Apple 均不予认可。

J. 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)，则可获取回应信息。

K. Apple Store 零售店闭路电视数据请求

闭路电视数据可能因商店位置而异。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。仅针对 CCTV 数据的请求可发送到邮箱：lossprevention@apple.com。政府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。

L. 游戏中心

游戏中心是 Apple 的社交游戏网络。可能可以提供有关用户或设备的游戏中心连接信息。申请者所在国家的具有 IP 地址和交易记录的连接日志 (如有) 可能可以通过提交适当、合法、有效的请求来获取。

M. iOS 设备激活

当客户激活 iOS 设备或升级软件时，根据事件情况，从服务提供商或设备向Apple 提供某些信息。可能可以提供事件的 IP 地址、ICCID 号码和其它设备标识符。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：对于具有双卡功能的设备，可以通过传票或更大的法律程序获得 nano SIM 和/或 eSIM 的运营商信息 (如果有)。eSIM 是一种数字 SIM 卡，让用户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。更多信息请参见：http://support.apple.com/zh-cn/HT209044。

N. 登录日志

可以从 Apple 获得用户或设备对 Apple 服务 (例如：iTunes、iCloud、My Apple ID 和 Apple Discussions) 的登录活动 (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，则可以获取带 IP 地址的连接日志 (如有)。

O. “我的 Apple ID”和 iForgot 日志

请求方可能可以从 Apple 获取用户的“我的 Apple ID”和 iForgot 日志。“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，则可以获取带 IP 地址的连接日志 (如有)。

P. 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 数据时解密这些数据。Apple 无法拦截 FaceTime 通信。在用户发起 FaceTime 电话邀请时，Apple 会生成 FaceTime 电话邀请日志。这些日志并不表示用户之间实际发生了任何通信。FaceTime 电话邀请日志最多保留 30 天。请求方可能可以通过法院命令、调查函或国内同等法律文书来获取 FaceTime 通话邀请日志 (如有)。

Q. iMessage 信息

iMessage 通信是经过端到端加密的，Apple 无法在设备之间传输 iMessage 数据时解密这些数据。Apple 无法拦截 iMessage 通信，而且 Apple 没有任何 iMessage 通信日志。Apple 确实有 iMessage 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功能查询日志不表示用户之间实际发生了任何通信。Apple 无法根据 iMessage 功能查询日志来确定是否发生了任何实际的 iMessage 通信。Apple 也无法识别发起该查询的实际应用程序。iMessage 功能查询日志不确认是否实际尝试了 iMessage 事件。iMessage 功能查询日志最多保留 30 天。请求方可以通过法院命令、调查函或国内同等法律文书来获取iMessage 功能查询日志 (如有)。

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：否，设备不必向 Apple 注册也可运行或使用。

问：Apple 能否为我提供当前已锁定的 iOS 设备的密码？
答：不能，Apple 没有权限访问用户的密码。

问：你可以帮我将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。请包含设备的序列号或 IMEI 号以及任何其他相关信息。如果客户信息可用，我们将与客户联系并建议他/她联系执法部门以恢复设备。但如果通过提供的信息无法确定客户，您可以根据指示提交有效的法律请求。

问：Apple 是否会保留丢失或被盗设备的列表？
答：否，Apple 不会保留丢失或被盗设备列表。

问：当执法机构在结束调查/刑事案件后，应该如何处理相应信息？
答：在相关调查、刑事案件和所有上诉完结后，提供给政府或执法机构的包含个人可识别信息 (包含任何副本) 的信息和数据应销毁。

问：您是否会通知用户您接收到与他们相关的执法机构信息请求？
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账户请求。Apple 将会通知客户和账户持有人，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可能会给公众造成严重的伤害或死亡的迫在眉睫的风险，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，Apple 合理地认为提供通知可能会妨碍司法公正或破坏司法管理。