法律程序指南

美国境外的政府和执法机构

本指南旨在供美国境外的政府和执法机构使用。此类政府和执法机构在相关国家或地区请求 Apple 实体提供有关使用 Apple 设备、产品和服务的顾客的信息时，应遵循本指南。Apple 在必要时会更新本指南。

在本指南中，“Apple”是指在特定地区或国家对顾客信息负责任的相关实体。作为一家全球性公司，Apple 在不同的司法辖区设有多个法律实体，这些实体将对由其收集并由 Apple Inc. 代其处理的个人信息负责。例如，美国境外的 Apple 零售实体中的销售点信息将由各个国家/地区的各个 Apple 零售实体控制。根据具体辖区内各项服务相关条款的具体规定，与 Apple.com 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，在澳大利亚、加拿大、爱尔兰和日本的 Apple 美国境外法律实体负责其各自所在地区内的 Apple 服务相关顾客数据。

所有关于 Apple 顾客信息的其他请求，包括与信息披露相关的顾客问题，都应该通过 www.apple.com.cn/privacy/contact/ 提交。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，并且会按照法律要求提供详细信息。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) 或根据依《澄清境外数据的合法使用法案》(Clarifying Lawful Overseas Use of Data Act) 订立的行政协议 (以下简称“CLOUD 法案协议”) 提出请求，则符合 ECPA 的规定。Apple 仅在回应此类合法的有效流程时才会提供顾客账户中保存的顾客内容。

对于私人机构请求，Apple 遵守适用于控制顾客数据的当地实体的法律，并会按法律要求提供数据。

Apple 制定了一个集中管理流程，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。收到的所有请求都将由我们法务部门中一支训练有素的团队负责审核和评估；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，则会反对、质疑或拒绝该请求。

Apple 通过提出请求的官员的执法机构官方电子邮件地址向提出请求的执法机构提供回应。提出请求的执法机构负责保存有关 Apple 所提供回应的所有证据。

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 touch、Apple TV、Apple TV+、Apple Watch、HomePod、AirPods、AirTag、各种消费类和专业软件应用程序、iOS 和 macOS 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。Apple 根据 Apple 隐私政策以及适用于特定服务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，我们不会提供关于 Apple 顾客的信息。

Apple 在向美国境外的政府和执法机构披露电子信息时，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 (以下简称“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。如果您选择向以上邮箱发送电子邮件，则应该通过政府或执法机构有效的官方电子邮件地址发送。

向 Apple 提出的法律请求应旨在获取特定 Apple 设备或顾客的相关信息，以及 Apple 向该顾客提供的特定服务的相关信息。只有当 Apple 根据其数据保留政策仍然保有所请求的信息时，Apple 才可以提供 Apple 设备或顾客信息。Apple 会保留在下文“可以提供的信息”部分某些小节中所列的数据。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、反对、质疑和/或拒绝。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) 或根据依《澄清境外数据的合法使用法案》(Clarifying Lawful Overseas Use of Data Act) 订立的行政协议 (以下简称“CLOUD 法案协议”) 提出请求，则符合 ECPA 的规定。Apple 仅在回应此类合法的有效流程时才会提供顾客账户中保存的顾客内容。

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，恕不另行通知政府或执法机构。

II. 向 Apple 提出的法律请求

A. 政府和执法机构的信息请求

Apple 接受政府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表》模板，然后通过政府或执法机构的官方电子邮件地址将该表直接发送至 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 5 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，则这些标识符应以可编辑的格式 (例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 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。

请注意：由于系统安全标准，Apple 不会通过电子邮件中提供的任何链接下载法律请求或相关文件。

为使 Apple 能够应执法机构请求披露顾客信息，提出请求的执法人员必须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)、lettres de réquisition ou commissions rogatoires (法国)、Solicitud Datos (西班牙)、Ordem Judicial (巴西)、Auskunftsersuchen (德国)、Obligation de dépôt (瑞士)、個人情報の開示依頼 (日本)、Personal Data Request/Orders/Warrants/ Communications Data Authorisations (英国)，以及来自其他国家/地区具有同等法律效力的法院命令和/或请求。

B. 管理及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有效的法律依据；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。

考虑到处理能力和系统限制的影响，Apple 无法接受涉及 25 个以上账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 个以上账户标识符，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重新提交新的法律请求。

C. 保留请求

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》(Mutul Legal Assistance Treaty) 或根据依《澄清境外数据的合法使用法案》(Clarifying Lawful Overseas Use of Data Act) 订立的行政协议 (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。

保留请求必须注明相关的 Apple ID/账户电子邮件地址，或使用目标 Apple 账户的顾客的全名**和**电话号码，以及/或者全名**和**实际地址。收到保留请求后，Apple 将对提出请求时可提供的现有顾客数据进行一次性数据调取，并保留 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。如对同一账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

如果提出的请求与涉及紧急和严重个人生命/安全威胁、国家安全或重要基础设施/装置安全的情况有关，则 Apple 会将该请求视为紧急请求。

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。

如需出于紧急情况请求 Apple 自愿披露信息，提出请求的政府或执法官员应填写《政府和执法机构紧急信息请求表》，然后通过其政府或执法机构的官方电子邮件地址将表直接发送至 exigent@apple.com，并在主题栏中注明“紧急请求”。

如果政府或执法机构通过填写《政府和执法机构紧急信息请求表》请求 Apple 提供相应的顾客数据，则 Apple 可能会联系负责提交《政府和执法机构紧急信息请求表》的政府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《政府和执法机构紧急信息请求表》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. 账户限制/删除请求

如果政府或执法机构请求 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 (包括有罪判决或令状)，证明要限制/删除的账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 (通常为有罪判决或令状)，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，采取必要措施来限制/删除该账户；同时将相关过程告知发出请求的机构。

F. 顾客通知

为了回应政府或执法机构提出的合法有效的请求而查询顾客的 Apple 账户信息时，Apple 会通知这些顾客，但以下情况除外：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可识别身份的个人带来伤害或死亡的风险；案件涉及儿童侵害；通知不适用于案件的基本事实。

90 天后，Apple 会就紧急信息披露提供延迟通知，但以下情况除外：法院命令或适用法律禁止提供通知；Apple 单方面认为提供通知可能会给可识别身份的个人或群体带来伤害或死亡的风险；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可识别身份的个人或群体带来伤害或死亡的风险，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 (通常为有罪判决或令状) 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 在因此而限制/删除相关账户时会通知顾客；除非存在以下情况：法律

程序本身、Apple 收到的法院命令、适用法律禁止提供通知；案件涉及儿童侵害；Apple 单方面有理由认为提供通知会给可识别身份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。

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 macOS 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 macOS 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。如果法律请求包含 5 个或更多序列号，则应按照 Apple 要求以可编辑的电子格式 (例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 提交这些序列号。

B. 顾客服务记录

Apple 可以提供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，我们可能还会提供有关设备、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 账户时，会提供基本顾客信息，例如姓名、实际地址、电子邮件地址和电话号码。此外，我们可能还会提供关于 Apple 媒体服务购买/下载交易及连接、更新/重新下载连接的信息。IP 地址信息可能仅限于最近 18 个月。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/账户电子邮件地址。如果无法提供 Apple ID/账户电子邮件地址，则需要采用全名**加上**电话号码和/或全名**加上**实际地址的形式向 Apple 提供 Apple 媒体服务顾客信息，以便识别目标 Apple 媒体服务顾客账户。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 (.PDF 格式和可编辑的格式，例如 Numbers 表格、Excel、Pages 文

稿或 Word 文档) 发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。此外，由于系统安全标准，Apple 不会通过电子邮件中提供的任何链接下载法律请求文件。

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/借记卡或充值卡交易。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 (.PDF 格式和可编辑的格式，例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。此外，由于系统安全标准，Apple 不会通过电子邮件中提供的任何链接下载法律请求文件。

E. Apple.com 订单

Apple 会保留有关 Apple.com 在线订单的信息，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.com 在线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.com 在线订单信息的请求可以包含相关的 Apple ID/账户电子邮件地址。如果无法提供 Apple ID/账户电子邮件地址，则应按照 Apple 要求以全名**加上**电话号码和/或全名**加上**实际地址的形式提供顾客信息，以便识别目标 Apple 账户。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取有关 Apple.com 在线订单的购买交易信息 (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 (.PDF 格式和可编辑的格式，例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。此外，由于系统安全标准，Apple 不会通过电子邮件中提供的任何链接下载法律请求文件。

F. 充值卡

Apple Store Gift Card 以及 App Store 和 iTunes 充值卡都有序列号。这些序列号有多种格式，具体取决于设计和/或发行日期等可变因素。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 Gift Card 以及 App Store 和 iTunes 充值卡的相关信息。如果法律请求包含 5 个或更多充值卡序列号，则应按照 Apple 要求将这些充值卡序列号以密码保护/加密的文档/文件形式 (例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。

i. Apple Store 礼品卡

Apple Store Gift Card 可用于在 Apple.com 或 Apple Store 商店中进行购买。可以提供的记录可能包括 Gift Card 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 Gift Card，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 Gift Card 信息 (如有)。

请注意：如果您的法律请求包含完整的 Apple Store Gift Card 数据，出于数据安全目的，Apple Store Gift Card 数据应以密码保护/加密的文档/文件形式 (.PDF 格式和可编辑的格式，例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。此外，由于系统安全标准，Apple 不会通过电子邮件中提供的任何链接下载法律请求文件。

ii. App Store 和 iTunes 充值卡

App Store 和 iTunes 充值卡可在 Apple Music、App Store、Apple Books 和 Mac App Store 中使用。Apple 可以借助序列号确定 App Store 和 iTunes 充值卡是否已经激活 (通过零售店销售点购买) 或兑换 (添加至 Apple 账户的商店余额)。

如果 App Store 和 iTunes 充值卡已激活，可提供的记录可能包括商店名称、位置、日期和时间。如果 App Store 和 iTunes 充值卡已兑换，可提供的记录可能包括 Apple 账户相关的顾客信息、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 充值卡，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 充值卡信息 (如有)。

请注意：如果您的法律请求包含完整的 App Store 和 iTunes 充值卡数据，出于数据安全目的，App Store 和 iTunes 充值卡数据应以密码保护/加密的文档/文件形式 (.PDF 格式和可编辑的格式，例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。此外，由于系统安全标准，Apple 不会通过电子邮件中提供的任何链接下载法律请求文件。

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者通过 Apple Pay 购买所涉及的完整信用卡/借记卡卡号。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 support.apple.com/zh-cn/HT207957。

对于在 Apple Store 商店或通过 Apple.com 完成的购买，要请求相应的交易数据，应按照 Apple 要求提供相关交易使用的设备主账户号 (DPAN)。DPAN 为 16 位，可从发卡行获取。注：DPAN 用于与商家的免接触式支付交易中，并不是实际的信用卡/借记卡卡号 (FPAN/付款 PAN)。付款处理系统会将 DPAN 转换为相应的 FPAN。Apple 可使用相关 DPAN 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，则可以获取这些记录 (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/账户电子邮件地址。

请注意：如果您的法律请求包含 DPAN，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（.PDF 格式和可编辑的格式，例如 Numbers 表格、Excel、Pages 文稿或 Word 文档）发送到 lawenforcement@apple.com，
并且密码应该通过另一封电子邮件发送。此外，由于系统安全标准，Apple 不会通过电子邮件中提供的任何链接下载法律请求文件。

H. iCloud

iCloud 是 Apple 的云服务，可帮助顾客通过各种设备访问自己的照片、文档等内容。顾客还可以通过 iCloud 将其 iOS 和 iPadOS 设备备份到 iCloud。借助 iCloud 服务，顾客可以设置 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。对于 Apple 可以解密的数据，Apple 将加密密钥保存在其美国数据中心。Apple 不会接收或保留用于顾客端对端加密数据的加密密钥。

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/账户电子邮件地址。如果无法提供 Apple ID/账户电子邮件地址，则应按照 Apple 要求以全名**加上**电话号码和/或全名**加上**实际地址的形式提供顾客信息，以便识别目标 Apple 账户。如果请求方仅提供电话号码，或是仅提供 Apple ID/账户电子邮件地址，则可以提供与这些要素相关的已验证账户的信息。

I. iCloud 可以提供以下信息：

I. 顾客信息

顾客设置 iCloud 账户时，可能会向 Apple 提供基本顾客信息，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。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)

顾客的账户保持活跃状态时，iCloud 会存储顾客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。对于 Apple 可以解密的数据，Apple 将加密密钥保存在其美国数据中心。Apple 不会接收或保留用于顾客端对端加密数据的加密密钥。

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) 或根据依《澄清境外数据的合法使用法案》(Clarifying Lawful

Overseas Use of Data Act) 订立的行政协议 (以下简称“CLOUD 法案协议”) 提出请求，则符合 ECPA 的规定。Apple 仅在回应此类合法的有效请求时才会提供顾客账户中保存的顾客内容。

II. 高级数据保护。

iCloud 高级数据保护是一项使用端对端加密来保护 iCloud 数据的功能，具有 Apple 最高级别的数据安全性。对于为 iCloud 启用了高级数据保护的用户，提供的 iCloud 数据可能有限。高级数据保护的更多相关信息请访问 support.apple.com/zh-cn/guide/security/sec973254c5f/web 和 support.apple.com/zh-cn/HT212520。

如果用户已经为 iCloud 启用了高级数据保护，iCloud 可以提供以下信息：

a. 顾客信息
顾客设置 iCloud 账户时，可能会向 Apple 提供基本顾客信息，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 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。

b. 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)。

c. 电子邮件内容和其他 iCloud 内容
对于已启用高级数据保护的用户，iCloud 会在顾客账户保持活跃状态时，存储顾客选择在账户中保留的电子邮件、联系人和日历内容。如果请求方提出在所在国家/地区合法有效的正当请求，Apple 可能会提供这些数据，因为此类数据存在于顾客账户中。这些有限数据由 Apple 存储并在服务器位置额外加密。对于 Apple 可以解密的数据，Apple 将加密密钥保存在其美国数据中心。Apple 不会接收或保留用于顾客端对端加密数据的加密密钥。

高级数据保护采用端对端加密，Apple 无法解密某些 iCloud 内容，包括照片、iCloud 云盘、备份、备忘录和 Safari 浏览器书签。在某些情况下，Apple 可能会保留与这些 iCloud 服务相关的有限信息，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)。

III. iCloud 专用代理

iCloud 专用代理是一种互联网隐私保护服务，作为 iCloud+ 订阅的一部分提供。专用代理可保护用户在 Safari 浏览器中的网页浏览、DNS (域名空间) 解析查询以及未加密的 http app 流量。用户必须拥有 iCloud+ 订阅以及装有 iOS 15、iPadOS 15 或 macOS Monterey (macOS 12) 或更高版本的设备才能使用 iCloud 专用代理。有关专用代理的更多信息，请参阅 support.apple.com/zh-cn/HT212614 和 www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF。

启用专用代理后，用户网页浏览请求将通过两次独立、安全的互联网中继来发送。用户网络提供商和 Apple 运营的第一次中继能够看到用户 IP 地址。用户 DNS 记录将被加密，因此任何一方都无法看到用户尝试访问的网站地址。由第三方内容提供商运营的第二次中继会生成临时 IP 地址，将用户请求的网站名称解密，并将用户连接到相应网站。专用代理会验证连接的客户端是 iPhone、iPad 还是 Mac。专用代理会将用户的原始 IP 地址替换为从该服务使用的 IP 地址范围内分配的一

个 IP 地址。所分配的中继 IP 地址可由同一区域的多个专用代理用户共享。

如果用户浏览网页请求使用了专用代理，则 Apple 无法通过专用代理 IP 地址确定用户客户端 IP 地址或相应的用户账户。Apple 无法提供有关与专用代理 IP 地址关联的 AppleID 的信息。

注：iCloud 专用代理仅在部分国家或地区提供。如果用户启用了专用代理，并且前往不提供专用代理的地方旅行，这项功能将会自动关闭；当用户返回支持专用代理的国家或地区时，这项功能会重新自动开启。

I. 查找

“查找”是一项由用户启用的功能，通过该功能，iCloud 顾客能够找到其丢失或遗忘的 iPhone、iPad、iPod touch、Apple Watch、AirPods、Mac 和 AirTag，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。有关此服务的更多信息，请参阅 www.apple.com/cn/icloud/find-my/。

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 设备丢失或失窃，可访问以下支持链接了解相关信息以及可以采取的措施：support.apple.com/zh-cn/HT201472。

“查找”连接日志的有效期为 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. AirTag 和“查找”网络配件计划

顾客只需将 AirTag 挂到个人物品上，或使用“查找”网络配件计划中的产品，即可借助 iPhone、iPad、iPod touch 和 Mac 上的查找 app 轻松找到相应的物品。

利用 AirTag 以及运行 iOS 14.5 和 macOS 11.3 或更高版本的设备，顾客在寻找丢失的个人物品 (如钥匙、背包、行李等) 时就能使用查找 app 获得帮助。AirTag 必须在配对 iPhone、iPad 或 iPod touch 的蓝牙信号范围内，才能播放声音或在兼容的 iPhone 机型上使用精确查找功能。如果 AirTag 不在物主身边，可以利用由全球数以亿计的 Apple 设备组成的“查找”网络；这个网络中在它附近的设备可以提供 AirTag 的大致位置。更多信息请参见： support.apple.com/zh-cn/HT212227 和 support.apple.com/zh-cn/HT210967。

“查找”网络配件计划已向第三方设备生产企业开放了“查找”网络，以便其产品 (自行车、耳机等) 也能使用这项服务，这样，顾客就能用运行 iOS 14.3 和 macOS 11.1 或更高版本操作系统的设备，通过查找 app 找到受支持的第三方产品。

要将 AirTag 或受支持的第三方产品添加到查找 app 的“物品”标签页，顾客必须使用 Apple ID 登录到自己的 iCloud 帐户，启用“查找”功能，然后将 AirTag 或受支持的第三方产品注册到其 Apple ID。整个交互过程经过端对端加密，Apple 也无法查看任何 AirTag 或受支持第三产品的位置。更多相关信息，请参阅： support.apple.com/zh-cn/HT211331。

在知晓序列号的情况下，如果请求方提出在所在国家/地区合法有效的正当请求，Apple 可以提供配对账

户的详细信息。AirTag 配对历史记录的有效期为 25 天。以下支持链接提供了查找 AirTag 序列号的相关信息： support.apple.com/zh-cn/HT211658。

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。如果法律请求包含 5 个或更多序列号，则应按照 Apple 要求以可编辑的电子格式 (例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 提交这些序列号。

K. 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。

L. IP 地址请求

在提交以 IP 地址作为识别符的法律程序之前，Apple 要求执法部门确定主体 IP 地址不是公共 IP 或路由器 IP 地址且不使用运营商级别网络地址转换 (CGNAT)，并在法律程序送达期间向 Apple 确认它是非公共 IP 地址。此外，此类请求必须包含不超过三天的日期限制。为了响应此类请求，Apple 可以生成连接日志 (请参阅下文第 III.Q 部分)，让执法部门可尝试从其中识别特定的 Apple 账户/Apple ID，以便在后续法律程序请求中用作识别符。如果请求方提出在所在国家/地区合法有效的正当请求，则可以获取基于 IP 地址的 Apple 顾客数据 (如有)。

M. 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 接口) 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)。

N. 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。如果请求仅涉及闭路电视数据，可发送至 lawenforcement@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。

O. 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，则可以获取连接日志 (如有)。

P. 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 编号和其他设备标识符。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，请参阅：support.apple.com/zh-cn/HT209044 在中国大陆、香港和澳门，iPhone 12、iPhone 12 Pro、iPhone 12 Pro Max、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。

Q. 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)。

R. “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)。

S. FaceTime 通话

FaceTime 通话经过端对端加密，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 通话通信。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)。

T. iMessage 信息

iMessage 信息通信经过端对端加密，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，并将其发送到 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 信息功能查询日志并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)。

U. Apple TV app

顾客可使用 Apple TV app 浏览、购买、订阅和播放 Apple TV+、Apple TV Channels、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/账户电子邮件地址。如果无法提供 Apple ID/账户电子邮件地址，则需要采用全名加上电话号码和/或全名加上实际地址的形式向 Apple 提供顾客信息，以便识别目标顾客账户。政府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，此类数据应以密码保护/加密的文档/文件形式 (.PDF 格式和可编辑的格式，例如 Numbers 表格、Excel、Pages 文稿或 Word 文档) 发送到 lawenforcement@apple.com，并且密码应该通过另一封电子邮件发送。此外，由于系统安全标准，Apple 不会通过电子邮件中提供的任何链接下载法律请求文件。

V. 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，顾客可设置账户并使用自己的 Apple ID 登录。顾客无需使用社交媒体账户，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，请参阅 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：可以，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：设备是否必须向 Apple 注册才可以正常使用?
答：不，设备无需向 Apple 注册也可运行或使用。

问：Apple 可以提供我当前锁定的 iOS 设备的密码吗?
答：不可以，Apple 无权访问顾客的密码。

问：Apple 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，可以联系 lawenforcement@apple.com。请在您的电子邮件或任何其他相关信息中注明设备序列号 (或 IMEI，如有)。有关查找序列号的信息，请参阅： support.apple.com/zh-cn/HT204308。

如果有顾客信息，Apple 将与顾客联系，提供执法部门的联系信息，以便顾客重新获得设备。但如果无法通过提供的信息确定顾客，您可以按照相关说明提交有效的法律请求。

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

问：如果执法机构结束了调查/刑事案件，应该如何处理 Apple 为回应相关请求而提供的信息?
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账户请求。Apple 将会通知顾客和账户持有人，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会给个人带来严重伤害或死亡的直接风险、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。