ASIAN AMERICANS ADVANCING JUSTICE AAJC

构建数字防御工具包

2026年指南

01 明智地使用电话、短信和电子邮件的各种服务

为了防止执法部门读取您的通话和短信历史记录，请使用Signal或Hushed等应用软件（apps），这些软件无须连接您的个人电话号码连，**且具有端到端加密（E2EE）功能。**

您可以在KaKao Talk和Telegram等平台上打开**“秘密聊天”来启用E2EE。**

在发送敏感文档时，创建一个辅助电子邮件帐号，此账号和您个人电子邮件地址之间不设链接。

一些电子邮件提供商可能会与广告商或执法部门共享您的数据。请注意以下文字：

“‘我们可能会与合作伙伴共享数据’，或‘我们扫描电子邮件以改善我们的服务’”

02 采用社交媒体的最佳操作

将您的帐号设置为私人账号，以限制能读取您的帖文、朋友圈和位置的人群，关闭自动位置追踪，**以及避免共享生日或工作地点等个人信息。**

美国国土安全部（DHS）政策的最新发展允许移民执法人员审查您5年前的社交媒体活动。

03 限制在线追踪和定向广告

您是否收到过来自国土安全部关于"自我驱逐"的广告？您看到的产品价格是否比别人更高？这说明您正在被追踪。

选择退出社交媒体上的个性化广告，禁用手机上的移动广告ID，删除apps位置许可，并每次都点击“拒绝Cookies”。**在访问诊所、法律办公室或参加抗议活动时，始终关闭位置服务。**

04 在旅行或参与敏感活动时请使用数字安全技术

如果你需要使用导航到达目的地，请使用不需要互联网连接的离线地图应用apps。

请注意，**自动车牌阅读器（ALPR）可以跟踪您的汽车行驶跨越州界线；**考虑使用公共交通或出租车。

关闭面部识别和指纹扫描——如果你的手机被扣押，执法部门可以使用以上技术来解锁你的手机，但他们没法得到你的密码解锁。

隐私保护通常由边境巡逻人员酌情决定。

在评估个人旅行风险时，请考虑政治气候和当前的新闻周期。

05 谨慎使用人工智能聊天机器人

切勿将个人信息输入人工智能聊天机器人的软件中，例如您的姓名、地址、案件详情、移民身份或身份信息。

聊天历史会被存储，并可用于训练未来的模型。

而不是问：“我没有证件，如果ICE来我家，我需要知道我的权利。”

可以问ChatGPT：“如果遭遇美国移民和海关局执法局（ICE）人员，移民的一般权利是什么？”

06 谨慎使用监控摄像头与智能家居设备

智能家居设备可能会允许未经授权的用户及执法机构在您不知情的情况下获取敏感视频、**录音或设备控制功能。**

定期检查设备权限，看看谁有权访问您的摄像头和智能扬声器，或可考虑拆除全部智能家居设备。

07 考虑你在公共场所的隐私

在政府大楼、公交车站、购物区和边境地区等公共区域，监控都非常普遍。请注意，**执法部门可以使用监控摄像头、车牌阅读器、面部识别等技术，**甚至附近的无线网络来识别您的身份。

ICE正在使用面部识别应用程序来加快移民拘捕。

请注意，这些工具在亚洲人脸上的识别准确率较低，这会导致错误拘捕。

如果你处于高风险情况，可以考虑戴口罩和帽子，在不使用蓝牙和WiFi时关闭它们，并避免可能正在拍照的他人在网上发布您的照片。