Strait News 海峡都市報 报料：智慧海都 968880
2025年3月14日 星期五 责编/林威 美编/建隆 校对/德峰

便捷背后存隐忧 手机智能助手

自动完成打车、导航……只要说说话，就可轻松调用APP，

N法治日报 广西新闻网

随着手机智能助手的出现，用户只需说出心中所想，就能轻松调用各类第三方APP，自动完成打车、导航、点餐、写评论、发微信等各种任务。这极大地简化了手机操作流程，让生活变得轻松又高效，但与此同时，关于信息暴露、隐私裸奔以及安全隐患的质疑声也不绝于耳。

专家介绍，不少手机智能助手主要通过AI多模态大模型，在绕过第三方APP授权的基础上，以识屏+模拟点击的方式来实现各种功能。虽然实现了便捷的操作，但也带来了巨大的隐私风险，如遭遇黑客攻击、用户数据泄露、转移账号资金等。

建隆漫画

使用 需开启无障碍服务权限 可监控手机上全部应用

记者尝试发现，有的手机智能助手需要用户授权开启无障碍服务权限，有的则默认开启无障碍服务，更有甚者，没有提供关闭无障碍开关的选项。

据了解，无障碍服务，是安卓系统为残障人士精心打造的一项贴心功能，旨在让他们也能像普通人一样便捷地使用智能手机。通过这项服务，视障人士可以借助屏幕阅读器“听”到屏幕上的文字信息，从而实现与手机的交互；行动不便的人士则可以利用自动点击等功能，减少手动操作的困难。

根据安卓无障碍服务的介绍，无障碍服务主要包括使用屏幕阅读器（即读屏）、更改显示设置（如放大屏幕、颜色反转）、互动控件（如开关控制、自动点击）、音频和字幕（如声音增强器、更改字幕格式）等。

这也意味着，无障碍服务可以监控手机上的全部应用，获取屏幕上所有的界面元素。

专家 给用户财产安全与个人隐私 带来风险

北京市君益诚律师事务所合伙人杨子江介绍，用户一旦开启无障碍服务，手机屏幕上的所有信息就会被手机智能助手获取，包括个人身份、聊天记录、地址乃至密码框内输入的内容。再加上无障碍服务的自动点击功能，用户的资金安全也可能岌岌可危。“这就像是在手机上开了一个‘后门’，他人可以随便进出，也可以顺手牵羊。”

“在智能助手以前，无障碍服务除了辅助残障人士，另一大用途实际上是在木马、外挂等非法软件上。一般来说，木马软件会伪装成正常APP，诱导用户在下载后开启无障碍服务。一旦开启，木马软件就会监控页面和键盘情况，窃取支付密码。随后木马软件会随时观察用户是否在使用手机（是否锁屏），如果一段时间未使用，木马软件就会自动点开钱包软件、转走资金。”杨子江说。

在北京潞丰律师事务所合伙人黄艳看来，无障碍权限虽然能为有特殊需求的群体提供实质性的帮助，但对于普通用户来说，还是应谨慎开启此类权限，因为系统对这些功能的调用限制相对较少，理论上它几乎可以执行所有的屏幕操作，容易引发数据滥用或过度采集信息的问题，给用户财产安全与个人隐私带来风险，还可能造成不正当竞争等市场秩序问题。

建议 谨慎授予权限 定期审查已授权应用

据了解，手机智能助手高度依赖云端大模型，大量的用户指令理解、截屏后识别屏幕的工作，不是在手机内完成，而是传输到云端处理。

对此，杨子江直言，这可能会带来更大的安全隐患，大量用户数据被手机厂商获取。这和所谓的“端侧大模型”相悖，也加大了数据泄露的风险。而且手机大模型的训练需要大量的用户数据，手机厂商是否会把截屏来的用户数据投喂给大模型做训练，投喂前是否经过了妥善的数据脱敏，用户也无从得知。

杨子江说，用户如果需要使用手机智能助手，应当注意充分了解开启无障碍服务后使用智能助手的网络安全风险；仔细阅读手机内智能助手相关的隐私政策，了解被搜集的数据范围、用途和存储路径；在使用时密切关注智能助手的动向，避免误操作；在使用后尽快关闭无障碍服务；涉及支付、转账等场景时尽量避免让智能助手辅助操作，关闭智能助手能调用的APP免密支付。

黄艳说，用户在使用手机助手时应当谨慎授予无障碍权限，注意授权权限，仔细阅读相关服务协议、隐私政策，并定期审查已授权的应用列表、账户设置中的隐私选项，及时撤销不再需要或可疑的应用权限、删除不必要的账户和数据，保持操作系统和应用程序的更新，使用加密和匿名工具等，理性使用社交媒体信息分享，以减少潜在威胁。

措施 提升告知同意流程的 透明度和有效性

在杨子江看来，手机智能助手的推广使用，需要经过APP和消费者的双重同意。手机智能助手应与其调用的APP合作，从该APP提供的接口调用和启动操作，配合APP的安全管控措施，并向消费者清晰告知其使用相关权限及是否可能存在数据泄露和安全风险。

杨子江说，为了确保消费者能够真正理解并自愿同意手机智能助手系统软件的用户协议和隐私政策，从而有效地行使对个人信息的控制权，应当对消费者信息的告知同意规则采取改进措施，提升告知同意流程的透明度和有效性。

“首先是明确手机智能助手系统软件的告知内容。需以简洁明了的语言制定用户隐私政策，并突出显示关键信息，如处理个人信息的主体、第三方共享情况、信息使用目的等。对于敏感个人信息，应在隐私政策中特别标注，并在每次收集时通过弹窗等形式明确获得用户同意。”杨子江说。

其次是优化用户的同意机制，采用明示同意方式，即用户通过主动点击“同意”按钮来表达对隐私政策的认可。可以考虑引入电子签名作为同意方式，以增强用户对其授权行为的重视。同时，根据信息敏感度的不同，可以采取差异化的同意策略，对于高度敏感的个人信息，则始终需要用户的明确同意。

黄艳说，手机智能助手在使用过程中涉及手机厂商、第三方大模型公司、APP、云服务等众多主体，数据在不同主体间流动，导致各方在用户隐私保护和数据安全上的责任关系难以区分，给监管带来挑战。虽然一些手机厂商已经在保护个人信息、化解用户隐忧上进行了一定程度的完善，但仍然存在数据用途说明不够清晰、普通用户难以充分认知隐私政策及潜在安全隐患、难以避免第三方滥用无障碍权限的风险等问题。

此外，现有监管法律法规如网络安全法、数据安全法、个人信息保护法、《网络数据安全管理条例》等虽然对新兴技术的数据处理活动作出了特殊规定，但在新技术应用初期，难免会存在一些模糊地带，仍然存在法律规制滞后的问题。

观点 完善立法加强监管

杨子江说，从市场环境和竞争的角度看，手机AI助手还可能涉嫌不正当竞争。第三方APP的流量入口转移到AI助手，而且APP本身的开屏广告、用户使用时长等营利机制均受到干扰，这很可能有损APP厂商的利益。

“AI助手未经授权利用现有APP的功能去开展服务，如同寄生在这些APP上搭便车，竞争秩序也可能因此被扭曲。为确保合规，宣称第三方APP零适配的AI智能体厂商，同样有必要获得第三方APP公司的授权。”杨子江说。

黄艳说，手机智能助手推广使用的健康发展，离不开技术更新、行业自律、完善监管等方面的协同治理。一方面，企业应当加强技术研发，完善用户数据处置流程的合法合规性，构建更加智能化的内部防御系统，实时监测和拦截潜在的网络攻击和数据泄露风险，提高用户数据的安全性和隐私保护水平。另一方面，职能部门应积极出台相关政策、加大法律规制和监管力度，厘清手机厂商、第三方大模型公司、APP、云服务等各方在用户数据安全保密方面应承担的责任，防范应对智能手机助手使用带来的隐私泄露风险。

声音 莫让“便捷”成“便窃”

在数字时代，手机智能助手成为人们生活的得力“小帮手”，动动嘴就能打车、点餐、发消息，极大地提升了生活效率。可这份便捷背后，却藏着隐私泄露、资金被盗的风险，“便捷”一不小心就可能沦为“便窃”。要想让手机智能助手健康发展，技术更新、行业自律、完善监管，一个都不能少。

技术革新是筑牢安全防线的关键。手机智能助手本是提升生活品质的好工具，不能因为安全隐患变成人人喊打的“过街老鼠”。只有企业在技术上发力、行业自律成风、监管严格到位，多方协同治理，才能堵死智能手机的“漏洞”，让便捷真正为人们所用，而不是成为侵害隐私与安全的“帮凶”，让大家安心享受智能生活带来的美好。

印刷：晋江市梅岭南路507号福建日报社（泉州）印务有限公司 电话：0595-82033695