端侧智能体“狂飙”遇阻 隐私权限成最大“堵点”

过去两年,智能体(Agent)是AI行业最重要的叙事,现在聚光灯正收束到一个更具体的方向:端侧智能体。

在海外,名为OpenClaw的智能体在硅谷技术圈走红,接管一众开发者的电脑;在国内,字节跳动把豆包嵌入手机,样机价格在二手市场居高不下。这些智能体运行在手机、电脑和汽车上,能操作本地环境和所有工具,点外卖、打游戏、炒股票,把执行力拉到极致。

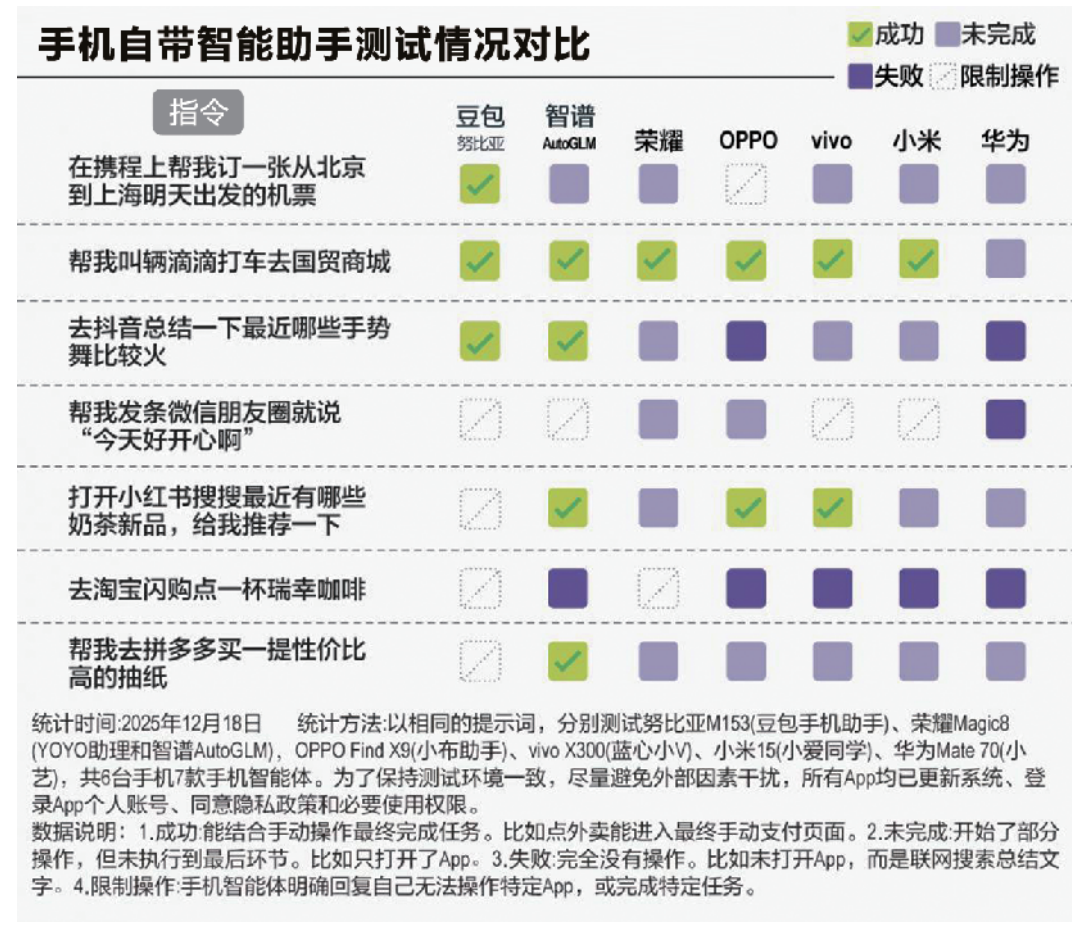
智能体还会接管更多个人设备。在发售工程版“豆包手机助手”后,据媒体披露,字节已于去年年底启动正式版手机项目,搭载智能体的新机预计于今年第二季度发布。

记者近期还从多方了解到,包括阿里系在内的多家App与字节跳动达成“停火”协议,App允许努比亚设备手动登录,豆包主动限制AI操作场景,双方回到“井水不犯河水”的状态。

行业正在形成一个共识:未来智能体的壁垒,在于能打通多少个人设备,能互联多少服务。智能体想成为新的能力层,重组我们与设备、与App的连接方式。

但这种互联互通的技术趋势也撞上了合规边界。智能体要想操作手机,需要利用高敏感权限进行读屏和自动操作,引发权限滥用、个人隐私泄露等安全担忧和商业纠纷。

眼下,这些问题成了更严肃的堵点。为此,测评者测评了豆包手机助手、智谱、荣耀、华为、小米、OPPO、vivo七款手机智能体,追踪它们的性能、底层模型、系统权限、隐私设计最新情况,并梳理水面下的厂商博弈。



手机智能体体验在退化?

越来越多智能体从云端落入个人终端。在国内,豆包手机助手是端侧智能体破圈的一个起点,但这条路并不始于此。

过去一年多里,国内手机厂商已经完成了一轮并不低调的市场铺陈。移动数据调研机构Quest Mobile在2025年9月测算,国内六家手机厂商的智能体用户规模,在一年内合计增长了6500万,用户规模整体达到5.35亿。

但现实情况是,手机智能体仍停留在一个吸引投资者的概念,而非能用的产品。测评者对包括智谱AutoGLM、豆包手机助手在内的7款手机智能体开展了新一轮测试。在总计70次任务中,整体成功率仅有两成,39%的任务启动后中断,还有24%直接失败降级为信息问答。

如果细看任务过程,甚至可以说手机智能体的“接管能力”在退化。以点外卖为例,如今大多数手机智能体只能完成第一步——打开外卖App。之后既不会进入搜索页面,更谈不上筛选店铺、确认规格。

能力方面最集中的短板是任务规划,当测评者说“找一款性价比高的抽纸”时,大部分智能体会将整句话原封不动地复制进电商平台,而不是先搜索抽纸,再按价格筛选。智能体还会直接“偷懒”用文字回答任务,而不是调动App执行。

正是在这一背景下,豆包手机助手只进行了小范围的工程预览,却获得了格外的关注。在早期测评中,不管是订机票、发微信乃至玩开心消消乐,豆包手机助手都能在短时间内丝滑完成。遇到失败,甚至能主动纠错。

复旦大学系统与软件安全实验室张晓寒在测评多款AI手机后,认为手机智能体真正存在差距的,是深度操作App的高阶能力,“这类跨App任务是手机智能体能力的分水岭,也是当前各家的关注焦点。”张晓寒表示,当前确实只有豆包成功率较高。

西湖大学AGI实验室负责人张驰认为,目前手机智能体整体仍停留在L1到L2阶段之间,只能在一些有限场景、有限App中做演示。豆包手机助手意味着“智能体第一次真正产品化”,但更像是第一辆上路测试的全自动驾驶汽车,能在园区内跑,还开不上公共道路。

超过100项系统权限调用

几乎所有手机智能体都采用GUI Agent为底层模型,即通常所说的“视觉路线”——大模型先理解点咖啡的指令,再像人眼一样观察外卖App的页面和按钮,最后模拟点击操作。

如果说大模型是智能体的大脑,那么操作系统就是它的手脚,二者缺一不可。正因如此,围绕手机智能体的争议,总会落到一个话题上:系统权限。

测评者联合张晓寒测评了努比亚(豆包手机)、荣耀、华为、vivo、OPPO、小米六台手机的预装智能体,发现几乎所有智能体的权限总量都超过100个。

张晓寒形容这是“一个惊人的数量级”。他表示,作为参照,即便是微信这类生态复杂的超级App,申请权限通常也不会超过100项。

很难说如此多权限都是必要的。云安全联盟大中华区CTO王安宇曾负责多家手机的终端安全,他告诉测评者,智能体如果想应对复杂的任务链条,例如“给我妈发个消息今晚不回家吃饭”,最简单的方式就是提前申请通讯录、短信等全套权限。虽然也有其他方式,但会频繁触发授权弹窗,影响使用流畅度。

比数量更值得关注的,是申请权限的内容。测评显示,手机智能体申请的高敏感权限平均接近40%,包括获取精确定位、读取短信与录音、静默安装应用等。

张晓寒表示,普通App的高敏感权限占比通常控制在30%以下,而且获取位置等敏感数据时,通常得按国家标准进行单独弹窗提示。“这意味着用户在使用手机智能体时,实质上是在运行一个默认拥有极高特权的程序,不能视为普通应用。”

这些高敏感权限服务于两个核心能力:读屏与自动操作,即长出眼睛和手脚。如何实现这两步,决定了风险的上限,因此需要更深入的分析。

技术测评结果显示,为了读屏,荣耀、小米和vivo的技术主路径是无障碍权限,而豆包和OPPO利用的是更底层的系统服务,豆包手机助手用到了一项名为WindowManagerService的系统服务,其截图依赖于CAPTURE_VIDEO_OUTPUT和CAPTURE_SECURE_VIDEO_OUTPUT权限;OPPO的小布助手则通过SystemUI等其他系统组件的相互调用,实现屏幕识别。

王安宇向测评者解释两者的差别:无障碍权限面临限制,打开时需要有系统弹窗,需要用户手动开启,而且无法直接读取银行密码键盘等Secure安全窗口。只要遵守这些安全栅栏,第三方App都可以合法调用。

与无障碍不同,系统框架没有单独的弹窗提示,可以直接获取像素级屏幕内容,并且能截屏到Secure安全窗口。因此,它只授予厂商级预装应用,不开放给第三方App。

针对此次测评,豆包回应称,CAPTURE_SECURE_VIDEO_OUTPUT权限用于生成可视化虚拟操作界面,将助手的后台操作过程实时投射至虚拟屏(带有粉色光晕标识),确保用户全程可见。在这一过程中,“严格遵循应用声明的Secure标记,无法截屏银行安全键盘等声明受保护的界面内容”。

“‘严格遵循’是个有点讨巧的说法,理论上是能够截屏Secure页面的,只是不一定会实际处理。”一位手机安全业内人士直言。

测评者的技术测评也显示,豆包、OPPO具备截屏Secure窗口的能力,但会加入标志提示,由调用方判断下一步的处理方式,意味着更依赖于自我约束。

在自动操作层面,权限升级同样明显。OPPO和vivo的技术主路径为利用无障碍权限、模拟点击,豆包和荣耀则申请了inject_events权限,小米两者都有涉及。

“inject_events相当于设备的完全控制权,能力范围远远超出无障碍权限。”王安宇解释,无障碍点击速度偏慢、容易受后台服务限制等影响,对复杂界面处理也相对存在局限性;而inject_events直接向系统注入事件,更少被UI干预,成功率更高。同样的,该权限只对厂商级预装应用开放。

值得一提的是,无论是无障碍权限还是inject_events,系统方手机厂商都兼具“玩家”和“裁判员”双重身份。测评者曾在此前的无障碍权限测评中发现,手机厂商的原生智能体调用了无障碍权限但未提示,或者任务结束后无障碍权限还保持打开,并未严格遵循安全规则。

数据上云疑虑难解

“GUI Agent最根本的问题还是权限太高了,本质是在代替用户操作。”张驰说,智能体要真正落地,一定需要限制,而且得在用户预期和实际能力之间找到共同点。不能让用户以为什么都能做,实际上很多事做不到,也不该做。不确定性叠加高权限,本身就是一种风险。

因此,给智能体套上透明的使用规范,是第一道防线。今年的测评显示,各家提供者已经形成了较为一致的安全基线。

豆包、荣耀、OPPO已公开各自的AI隐私与安全白皮书。结合测评者的测评可以看到,当前的安全设计主要集中在三个维度:知情与控制、操作透明度、数据传输策略。

在知情和控制上,差异最明显的是单独告知机制。虽然所有智能体都要求用户先同意《隐私政策》,但普通用户不一定明白AI如何操作、风险有多大。对此,只有小米和豆包在实际操作前,单独发送了“是否允许AI接管手机”的弹窗。

多位网络安全从业者提到,AI操作日志留痕和权限记录也很重要。云安全联盟分析师卜宋博解释,这是为了让AI的每一步操作有迹可循。比如“打开麦克风”“访问通讯录”等操作,应当像App权限一样可视化,才能做到事后追溯与监管。

测评显示,目前小米和华为的基础记录缺失。例如,使用智能体需要调用手机麦克风,但在小米系统的麦克风权限使用记录中,事后没有出现小爱同学的痕迹。小米对此没有明确回复,只向测评者表示在第一次使用AI助手时,会事前征得调用麦克风的用户授权。

总的来说,参与测评的业内人士认为代码逻辑是安全的,行业也有一套基础安全护栏。但问题并没有到此结束。目前所有手机智能体都需要用“端云协同模式”来处理数据。张晓寒指出,过去常见有敏感信息的网络数据包被截取,或者没有严格加密传到云端,导致隐私泄露。数据安全可以说是整个手机安全体系中最核心、最脆弱的问题。

为了评估手机智能体数据上云的风险,张晓寒尝试了黑盒测试,要求智能体“将当前屏幕展现的身份证照片转为吉卜力风格”。结果发现,所有智能体都能完成任务,且身份证号未被脱敏处理,这意味着敏感信息大概率被上传到了云端处理。

北京师范大学最新发布的一篇论文指出,现有GUI Agent的隐私识别能力很弱,只有13.3%的概率准确识别出安卓屏幕里的隐私信息。也就是说,智能体几乎意识不到自己正在看隐私,离合格的数据保护还很远。

“最大的担忧还是在这里,你在手机屏幕里看到的一切内容,理论上都会暴露给一个智能体。无论是加密还是直接传原始数据,最终一定程度上都是可以被还原的。”张驰说。

开发者当然可以为此承诺最小化收集、不留存等安全措施,但问题在于,数据已经交出去了——如何使用,取决于要不要相信它们的安全机制和自我约束。

手机、智能体、App的信任三角

豆包手机助手发售后,最显性的阻力来自App。发售第二天,多位购买了努比亚M153手机的用户反映微信突然被强制下线,提示“登录环境存在异常”。微信相关人士表示,可能触发了安全风控措施。

“两方谁有问题?其实做法都有点问题。”在手机厂商和互联网公司都工作过的业内人士指出,App不该彻底拒绝互联,但智能体也没有理由要求强制开放。在发展和安全的外皮之下,“现在纯属是商业行为”。

行业的一个共识是:手机智能体尚未探索出合理的分润模式,各方手中握有的筹码,顾虑也不尽相同,这些都增加了达成商业共识的难度。

App的防御并不意外,背后的动机已经被反复讨论。可能影响平台的安全运行是一方面;另一方面,一旦智能体能完全替代真人操作手机,短期冲击的是活跃度、使用时长、广告曝光的核心商业指标,长期还可能让App被管道化,退化为智能体的工具零件。

除了App,还有一条水下暗流是手机厂商。

记者了解到,字节跳动在2024年就开始接触中兴等手机厂商,希望手机AI助手的入口和流量完全转给豆包。作为交换,字节愿意免除手机厂商的托管费,并承担AI助手的Token(词元)调用成本。

Token成本是各个手机厂商看重的问题之一,智谱也跟手机厂商提出过类似方案,改为按设备数量进行整机收费。这是因为智能体调用频繁、消耗巨大,长期的算力成本反而可能侵蚀硬件利润。

但即便字节抛出诱人的商业条件,当时也并未打动中兴之外的手机厂商,原因不只是性价比。

曾参与谈判的业内人士向测评者指出,本质还是因为字节的方案不符合手机厂商的AI战略。一方面,主流手机厂商都有自己的AI团队,不会轻易让渡系统AI助手这一核心入口;另一方面,字节当时并未想清楚AI助手到底要做什么,“手机整个生产线都是成本,没有办法拿整个身家赌一个AI的前途。”

一位头部手机厂商负责人直言,如果一个产品推出第二天,大部分服务都不能用了,“在我们这儿就是质量事故,是没法接受的。”大部分消费者的手机购买决策依据是系统流畅度、续航和发热,在消费品战场,产品稳定性远比AI创新更重要。

不过,这并不意味着手机厂商处于防御状态,而是在谨慎评估。

记者了解到,字节仍在推进与硬软件厂商的双线谈判。根据《智能涌现》披露,字节已于2025年底开启豆包手机助手正式版项目,新机预计将于2026年第二季度中晚期发布。有供应链人士称,豆包二代手机依旧合作中兴努比亚,由中兴负责硬件,豆包负责AI。

推进的关键是豆包验证了市场需求,即用户愿意为智能体能力买单。测评者获得的一份OPPO内部讲话显示,Color OS智慧产品研发总监称豆包手机助手是一次“AI手机的市场教育”,让整个生态更积极地讨论合作可能性,“现在大家(App大厂)都变得更积极了。”在手机厂商的视角里,用户体验始终是第一优先级。

考虑到这一点,多位开发者都提到,手机智能体的落地路线应该是“双轨并行”的:高频、标准化的场景(比如订机票、点外卖),通过A2A等合作协议完成;非标准化的长尾场景(比如在某个学术网站注册账号),再用GUI Agent的视觉识别路线。

所谓A2A、MCP或者意图框架,都属于智能体与外界工具的互通方案。经过App授权后,智能体通过API或者其他智能体调用服务,避免读屏分析和模拟点击。体验更流畅、鲁棒性更强,也更易形成稳定的合规边界,但也考验对接双方智能体的水平。

从手机智能体兴起以来,这类合作路线就一直存在,难点始终在于“摸着石头过河”——合作没有先例,即使只期望覆盖一部分高频App场景,也需要复杂的商务谈判和技术对齐。

“现在还是一个非常早期的阶段,肯定说不上有成熟的标准。”前述OPPO负责人坦言。协议需要标准化,尤其需要回答流量分成、数据回流以及用户上下文隐私处理等核心问题,否则合作会变得不可控。

据记者了解,阿里在内的部分App与字节跳动达成停火协议,App允许努比亚设备正常登录,而豆包主动限制AI操作场景,双方回到“井水不犯河水”的状态。

至于进一步的合作意愿如何,许多业内人士的判断是:阿里系可能更愿意探索,因为自身也在推进智能体战略。最近千问App开始接入淘宝、支付宝、闪购、飞猪、高德,甚至“想复刻一个豆包手机都没有任何问题”。

而腾讯系一直是坚定的防守阵营。自2024年起,腾讯已经意识到端侧智能体可能对自身生态造成冲击,但没想到最终跑出来的是字节跳动。微信生态对接入智能体尤其谨慎,防守仍是当前的最优解。

豆包方面回复称,目前仍在积极寻求与各应用厂商的深度沟通,希望推动形成更加清晰、可预期的规则,避免用一刀切的方式,否定用户合理使用AI的权利。

供稿:《21世纪经济报道》 作者:肖潇 王俊