

封面
深镜

『超级智能体』带来隐私泄露之忧：

豆包手机的『主人』是用户还是AI？

华西都市报封面新闻记者 边雪

想象一下这样的未来：你仅凭意念，就能如《爱、死亡与机器人》剧中角色那样操控机械巨兽的每个动作；你家的扫地机器人完全自主地工作，而你手中的智能手机，已进化成一个能自主思考、并跨越所有应用为你代劳的“超级智能体”——它能够理解用户指令，并在多个应用间自动操作。用户只需对着手机说：“帮我对比一下各大外卖平台上哪家的汉堡更便宜。”豆包手机助手便能理解需求，自动在屏幕上滑动、点击，完成比价并下单。

12月1日，搭载豆包手机助手预览版的努比亚M153工程样机，在少量发售后迅速售罄。一台官方售价3499元的工程样机，在二手市场被炒至万元高价；一个本应面向开发者的技术预览版，却引发全民关注。然而，首批用户就遇到了微信登录异常甚至账号被封的问题。

当我们惊叹于科技的“魔力”时，《爱、死亡与机器人》那些关于技术失控、身份迷思与伦理悖论的故事，已从屏幕上的寓言，转化为我们时代迫在眉睫的拷问。

1

首批用户体验

►使用期间存在隐私泄露风险

搭载豆包手机助手技术预览版的工程样机努比亚M153，官方售价为3499元，却被市场赋予了远超预期的价值。12月8日，记者注意到，这款工程机在二手市场上的价格被迅速抬高，部分全新未拆封机型报价一度飙升至12999元，溢价幅度惊人。被炒至天价的工程机，折射出市场对AI手机的超高期待。豆包手机助手的亮相，迅速点燃了市场的热情。

试图通过AI接管手机操作的“超级管家”豆包手机助手，展示了一种未来生活的可能性：用户只需发出语音指令，AI便能像一个数字管家，自动在屏幕上点击、滑动，跨越APP边界，完成发微信、点外卖等操作。

手机研发从业者于琦告诉华西都市报、封面新闻记者：“我是通过二手交易平台买到的技术预览版豆包手机，到手后进行了一些简单日常场景的测试，优势在于打通了很多本来闭源的生态，比如微信功能、外卖购物平台的使用。我跟别人聊天的时候，豆包也会把用户点击按钮前说的话给识别进去，这个手机的操作也存在手机内容隐私泄露的风险。”



交易平台上的豆包手机被炒到万元高价。（网页截图）

2

跨应用操作引争议

►用户担忧可能失去对设备的控制

“用户许可即不侵权”，这句简单的原则在AI时代遇到了前所未有的挑战。豆包手机的争议核心，正是围绕其系统级权限展开的。

豆包手机助手使用的INJECT_EVENTS权限，允许应用向系统注入模拟的用户输入事件。这使其能够跨屏、跨应用模拟点击事件，完成用户操作手机的任务需求。

“调用这类系统级权限，带来了两大核心风险。”北京汉华飞天信安科技有限公司总经理彭根指出，一是权限的无边界扩张——传统权限具有单一性和规定性，但调用INJECT_EVENTS或无障碍权限，相当于拥有整栋大楼的钥匙。二是行为主体的模糊化。AI成为实际操作主体，其操作速度远超人类反应速度，用户可能因此失去对设备的直接控制。

针对外界对隐私和安全的担忧，豆包手机助手多次回应称，该权限的使用建立在透明的管理体系之上，全程需要用户主动授权，且用户可以随时中断。记者发现，豆包方面发布的《豆包手机助手白皮书》强调：豆包手机助手以端云AI安全防护体系为架构基础，构建了一系列的具有创新体验的智能AI业务。豆包手机助手坚信，保障用户对数据的控制权是AI服务价值的前提。

3

遭遇“抵制”

►多个APP限制豆包手机助手访问

当AI试图打破应用壁垒时，却与现有平台的规则发生了正面冲

突。豆包手机助手的遭遇，揭示了AI“系统级接管”与移动互联网时代“APP反外挂机制”的碰撞。

记者注意到，在豆包手机助手发售仅两天后，便有用户反馈微信提示“登录环境异常”，甚至有用户称微信账号被封。在登录支付宝、淘宝等应用时受到限制。使用农行、建行等手机银行时，APP内出现强弹窗提醒，要求关闭豆包手机助手后再进行使用。

“AI智能体并非普通用户，它具备超强的计算能力和不可控性。”对外经济贸易大学法学院教授许可表示，对于APP平台而言，为了防止黑客攻击、保障实名制和资金安全，拒绝此类非自然人的访问请求具有正当性。

“就像一个银行客户把珠宝放在保险箱里。他授权朋友去取，也给了账号和密码。但如果这个朋友是带着一把枪去的，银行为了安全，当然有权拒绝他进入。”许可说。

从“视觉模拟”到“接口合作”，两种技术路径背后是不同的生态哲学。豆包手机助手引发的争议，实际上反映了AI手机发展的两条不同技术路径。

豆包此次展示的方案属于“视觉识别+模拟触控”。AI通过系统底层权限，像一只“无形的手”，直接模拟人类手指在屏幕上的点击和滑动。这种路径的优势在于泛用性极强，理论上只要是人能看到的界面，AI就能操作。

而目前行业内更为主流的则是“接口调用”。包括荣耀、OPPO、vivo等手机厂商在内，其AI助手在涉及微信、支付宝等敏感应用操作时，更多是选择通过与APP厂商合作，利用开放接口来实现功能。

对此，清华大学电子工程系信息系统研究所副所长王钺提出，应赋予智能体独立身份，建立区别于自然人的数据通路。王钺认为，如果为智能体单独设计接口，既能发挥其增值服务价值，又能实现有效管控。

4

责任归属模糊

►当AI替用户做决定算谁的责任？

当AI代替我们做出决定，责任的归属变得模糊不清。在技术路径的博弈之外，更深层次的讨论指向了未来数字世界的生态秩序：我们是否需要一个全知全能的AI来“接管”手机？

手机不仅是硬件，更是人连接数字空间的入口。许可也表达了对“接管”一词的警惕。如果任由AI智能体接管这一入口，意味着将风险高度集中化。

一旦这个超级智能体出现安全漏洞或逻辑错误，所有被其接管的应用，无论是社交、金融还是智能家居，都将面临系统性风险。

豆包官方已经采取了一些主动调整。12月5日，豆包手机助手发文称，将对AI操作手机的能力做一些规范化调整，包括限制在各类APP中用于刷分、刷激励的自动操作能力，进一步限制银行、互联网支付等金融类应用的代操作能力。豆包手机助手同时呼吁，希望能够与各方形成更加清晰、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。

外骨骼机器人
怎样安全走入
寻常百姓家？

泰山、黄山、长城等景区纷纷引入外骨骼设备，为游客提供登山助力；各类展会上，外骨骼替代拐杖帮助老年人行走的视频总能引发热议……今年以来，科技感十足的外骨骼机器人火爆出圈，万元以内的价格让很多消费者为之动心。

外骨骼真的好用、实用吗？应该如何挑选产品？围绕这些问题，记者进行了调研采访。

什么是外骨骼？作为一种可穿戴机器人系统，外骨骼一般佩戴于腰腿部，通过电机、传感器、控制系统等技术协作，为人体运动提供外部的动力，来增强、辅助或重建人的运动能力。

近日，到泰山旅游的万女士体验了一把登山外骨骼租赁服务，感到颇为惊喜：“穿戴简单，每走一步腿部都有向上的推力，能节省大约三分之一的体力，而且爬完山第二天腿也不酸。80元使用3小时的价格，性价比挺高。”

“随着生活水平提高，人们更加关心自己的健康。外骨骼能够减轻体力消耗、减轻腰腿劳损，市场前景广阔。目前，国内几家头部企业都在探索用人工智能技术提升外骨骼的运动态势感知和意图识别能力，从而更准确适配人体行走。”中国电科21所（电科机器人）机器人及核心部件研发中心主任王洪武说。

沈先生85岁的父亲曾做过骨盆手术，留下了走路时身体前倾、右腿拖地的后遗症。在网上看到外骨骼帮助老年人行走的视频后，沈先生为父亲购入了一台外骨骼机器人。

“体验感并没有那么‘完美’。现在，父亲的右腿能比之前抬高约2厘米，走平地和上楼梯比之前有所好转，但是下楼梯不仅没有助力，膝盖负担反而增加了。而且如果没有跟上机器的节奏，还要自身更加用力去保持平衡。”沈先生说。

对此，多位专家提示，消费级外骨骼设备不可代替医疗康养设备。目前消费级外骨骼更适于帮助具备完整运动能力的人节省体能，建议高龄老人和有中风、骨骼疾病等生理受限人群谨慎使用。

受访专家表示，目前外骨骼机器人还处于大规模市场化的初期，面临个性化适配难、成本高、标准法规不完善等问题。亟需建立统一的产品标准，优化完善技术短板，引导行业规范良性发展。

专家表示，未来，随着外骨骼在更多医院、康养机构和社区居家场景落地应用，不断积累的真实世界数据也将促进算法的优化迭代，推动产品的技术水平提升。

据新华社