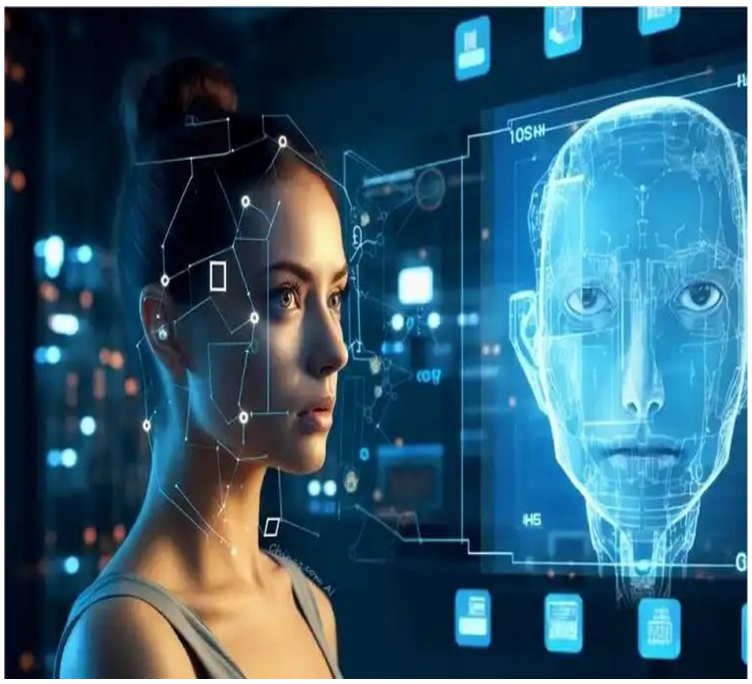
AI换脸风波引发一场公开听证



“公司虽然是2024年2月以我的名义在天津注册的，但我可以肯定，我没有注册过该公司，相关证件也没有丢失过，在此之前我都没去过天津。”当事人余某某说。

“当时从注册信息了解到，这家公司在登记时经过实名认证，注册人员是知情的……”天津市北辰区市场监督管理局代表说。

“余某某两张底档照片之间相隔5天，衣服、褶皱却完全一致；余某某底档照片与生活照片不一致……经上述照片的比对，发现存在AI换脸的严重可疑之处。”检察官说。

这是记者近日走进天津市北辰区人民检察院检察听证室看到的一幕，此时，余某某申请撤销公司登记行政检察监督案听证会正在进行。

当天上午9时，本案承办检察官、书记员、人民监督员、听证员及涉案一方市场监管部门代表进入听证室，因为当事人余某某远在广东，此次公开听证采取视频连线的方式进行。

记者注意到，公开听证颇有些庭审的“味道”——身份信息核实无误并宣布会场纪律后，听证主持人、北辰区检察院第五检察部主任王赞宣布听证会开始，书记员进行了听证权利义务告知。“是否申请听证主持人、书记员、案件参与人、听证员等人员回避”，王赞询问后，双方当事人均表示“不申请”。

经检察院调查核实：2024年4月25日，余某某缴纳个人所得税时，发现自己被冒名登记为天津某商贸有限公司的法定代表人、股东及财务负责人。后经核实，天津某商贸公司系在某App上申请公司登记，市场监管部门于2024年2月核准该公司登记，余某某被登记为该公司股东，认缴出资额200万元，持股比例100%，并担任法定代表人职务。

余某某向北辰区市场监管局申请撤销公司登记未果，又于2024年6月5日向法院提起诉讼，也没有达到目的。后该案进入北辰区检察院的检察监督程序。北辰区检察院主动践行新时代“枫桥经验”，就该案开展争议化解，于是就有了这次听证会。

“我没有注册过，证件也没有丢失过，甚至在此之前我都没去过天津。”余某某提出希望撤销这个公司登记。

北辰区市场监管局代表介绍，之前接待过余某某，当时从注册信息了解到，这家公司登记时是经过实名认证的，因此注册人员应当是知情的。根据《关于经实名认证登记企业当事人申请身份异议的处理意见》，针对通过实名认证程序登记后对身份有异议的，不适用撤销冒用身份信息取得登记工作程序，建议寻求司法途径解决。

随后，王赞出示了检察院依职权调取的证据，由双方当事人进行质证。第一组证据是余某某本人生活照片、天津某商贸有限公司注册时App后台保存余某某人脸识别底档照片以及同余某某类似在App注册公司的部分人员的底档照片。

王赞指出比对这些照片后发现的几点可疑之处：余某某两张底档照片之间相隔5天，衣服、褶皱却完全一致；余某某底档照片与生活照片不一致。经提请上级检察机关进行技术鉴别，得到的答复是从App后台调取的余某某人脸识别照片并非本人；余某某的底档照片与另案被虚假注册公司的当事人曾某波、曾某杰的底档照片进行比对，发现衣服颜色、褶皱完全一样，发型也一样，人脸不同。这样的比对结果，显著违背了生活常理。

第二组证据为检察官实地走访天津某商贸有限公司登记注册的地址位置照片，证实住址是虚假的。

第三组证据为天津某商贸有限公司注册时预留的“余某某2个电话号码”，调取机主信息发现，机主分别为聂某和高某，2个号码要么已欠费停机，要么是空号。

当事双方对证据无异议，听证员也进行了询问，主持人宣布休会，听证进入听证员评议程序。之后，听证员代表发表听证意见：“鉴于检察机关对案件的调查核实过程，证据展示环节，天津某商贸有限公司注册地址、预留手机号，还有余某某人脸识别照片系虚假的，存在诸多疑点和AI换脸风险，余某某很可能被冒名登记。需要市场监管局继续调查，如果真的存在冒名情况，应撤销。”

“冒名登记行为对我的工作和生活造成了严重影响，我也知道市场监管部门尽到了审查职责，但是我还是想能够切实解决问题，把我名下的公司给注销掉。”余某某说。

“我们回去后会将听证内容上报领导，认真调查研究、查找相关法律规定，请示上级单位，依法作出处理。”北辰区市场监管局代表说。

仅用时一个小时，听证会顺利结束。会后，王赞告诉记者，“今天的听证会不仅是对案件事实进行认定，更重要的是提供一个平台，促成行政争议化解，既能够减轻行政部门诉累，也可以帮助申诉人解决虚假登记面临的法律风险和经营困境”。

几天后，按照这次检察听证达成的共识，行政机关依法启动了撤销该公司注册的相关调查程序。

本报综合消息

把隐私作为卖点的AI手机 说得出做得到吗？

用户隐私已经成为AI手机与App之间的摩擦点。

有业内人士向记者透露，双方矛盾正在加剧。对于手机终端厂商，为完善AI功能，既需要第三方App的数据来补足手机本地数据，同时也需要App来落地用户任务，与App合作是最优解。但App厂商则抛出对用户隐私以及数据安全的担忧，以作对抗。

手机被瞄准作为人工智能落地应用的C端入口。2024年，各大厂商纷纷推出AI手机，根据IDC（国际数据公司）的预测数据，全球AI手机出货量预计达到1.7亿部，占市场总量的15%左右。

仅在上个月，OPPO就推出A5 Pro和一加Ace5系列几款AI手机，荣耀也对Magic5和Magic7系列AI手机进行了升级。

在许多手机发布会上，AI一键下单、AI帮点咖啡的场景触手可及。不过手机厂商在强调AI手机更快更强更懂用户的同时，也不忘强调自身对用户隐私保护的高度关注。

要实现合格的AI功能，直达用户心智，必须由数据到服务：丰富的用户数据、跨应用的调用、全场景的功能打通。因此，在这盘大棋局中，隐私保护与数据安全既是给予C端用户的承诺，也是B端多方的短兵相接之地。

在AI手机这幅全新的生态图里，用户数据在手机、大模型、App、云端流动，脚下是否埋着复杂雷区？这些问题不提前勘测和规避，可能会在AI手机时代大范围爆发。

数据隐私问题成各方“心病”

“我有些困了，帮我点杯喝的”，2024年10月，在荣耀MagicOS 9.0发布会上，荣耀CEO赵明用荣耀Magic7演示点咖啡。在收到这个指令后，YOYO智能体会根据以往记录判断赵明喜欢喝什么，然后自动打开外卖软件或小程序下单，并且这个功能是完全基于AI视觉，不需要第三方适配。

在会后的采访中，赵明反复强调没有数据保护和隐私安全的AI毫无价值。

用户隐私保护，已经成为所有手机厂商强调的重点。

探寻其原因，AI手机的很多服务需要获取用户的隐私信息才能够提供服务。

手机厂商的蓝图很美好：端侧的AI智能体可以成为用户“肚子里的蛔虫”——一句话、一个指令，便能顺畅给出想要的结果。用技术黑话来讲，就是立足于丰富的用户数据，全场景感知用户行为，叠加算法分析后，底层理解用户意思，最终以智能体作为端口实现服务触达。

要完成这一蓝图，打通第三方App是最重要的一块拼图。所以各个手机厂商纷纷释放自己的意图框架，希望第三方App开发者能共享自己的数据，更精准地判断用户意图，并让AI执行任务时实现跨App调用。

目前苹果、华为、荣耀、vivo等都发布了自己的意图框架方案。例如，华为的意图框架已开始商业化尝试，鼓励开发者接入。通过多种智慧分发入口华为系统能够接触到大规模的用户群体，涵盖了从亿级到千万级的不同层次；vivo也发布了意图框架白皮书，为行业提供了服务接入、流转与分发的全流程解决方案。

但一帆风顺的故事并不属于商业社会，说服第三方App加入手机厂商的意图框架并非易事。

App厂商的顾虑是，一方面，要开放自身的API接口，自身的数据安全是考量因素；另一方面，手机终端智能体直接调用App，可能抹去自身触达用户的机会，因此在商业层面亦有顾虑。

读屏成过渡方案，但问题还很多

这趟AI的列车，不占位就意味着掉队。端侧AI是目前落地应用的标准答案。于是，在难以打动App开放API的情况下，手机厂商也在尝试第二种路径：纯视觉形式。

简单理解，纯视觉形式就是“读屏”，智能体通过理解手机屏幕内容，模拟用户操作进行点击操作。

以一键点咖啡为例，根据兴业证券分析，手机智能体首先将用户的语音指令拆分理解，其次根据本地知识库收集用户日常习惯、给出相关的点单选项，根据手机时间、定位等信息填充配送地址；最后识别屏幕中的相关App，搜索咖啡品牌，识别并理解屏幕上的关键信息，进入外卖点单页面。

读屏的好处是，无需App厂商授权。“因为手机的操作系统天然会给予相关底层操作的权限，手机厂商很容易获取到读屏的‘特权’。”尚隐科技CEO张仁卓解释称。

但弊端也存在。“如果App突然设计结构改变、按钮位置变化，原来积累的算法又需要重新学习。”业内人士表示，“说白了如果能用API方式去解决，手机厂商肯定愿意用API方式去解决。”

可以说，读屏模式只能算是手机厂商眼下的过渡方案，仍有很多盲点有待厘清。

第一，读屏的方式如何保证数据安全是必须回答的问题。去年上新的微软AI“Recall”功能，因每隔几秒钟就对用户的活动屏幕进行截图而遭到强烈反对。此后微软回应称，所有Recall数据都存储在本地，并通过设备加密或BitLocker加密，并不会侵犯隐私。

第二，手机终端的智能体、大模型之间的数据链路需要厘清。目前，荣耀、华为、三星、OPPO、vivo、小米等头部厂商都已经发布自家大模型。并且，荣耀等厂商也为其他大模型提供入口，融入到其操作系统当中。不同任务可能由智能体分配给不同的大模型，是否涉及跨主体的数据调用，调用数据的权限如何厘清，如何授权？

第三，端云安全问题绕不过去。读屏的纯视觉路线需要识别手机屏幕内容，拆解需求，把图读一遍变成文字再来进行操作，对算力要求高，尤其是频繁大量操作的情况下。毕竟，如果AI智能体反应速度不如手工操作，也就失去了意义。但在端侧，功耗、内存等均是市场的考量因素，AI功能的实现，往往需要云端来实现。在2024年vivo开发者大会上透露的信息显示，vivo的每一步需要两秒左右，目前仍旧通过云端算力运行。

虽然机制上保证安全，但数据上云确实放大了风险。

于是，各个厂商纷纷强调自身的隐私保护措施。记者此前梳理发现，无论是苹果，抑或是国内的荣耀、vivo、OPPO，均采取优先本地化（端侧）处理+加密上传云端处理的措施。本地设备优先处理用户需求，当用户请求无法在端侧模型完成时，端云模型协同响应，加密上传云端模型处理，并有厂商强调“数据用完即删”。

与此前以App为抓手的隐私保护不同，AI手机的生态参与方更为复杂，其涵盖：手机终端、第三方大模型、App以及云服务等参与方，各方在数据流转的链路，以及责任关均需要厘清。不然就是死结，难以继续推进手机功能的完善。

根据Canalys预测，2024年全球市场AI手机渗透率达到17%，2025年更多中高端机型将配备更强大的端侧AI能力，推动全球市场渗透率达到32%，出货量接近四亿台。

在更强大的AI手机功能探索中，手机厂商希望为用户带来更智能、便捷和个性化的体验。比如，进一步深化多模态交互，将语音、文字、手势、表情、眼神等多种方式融合，让用户与手机的互动更加自然流畅；并将基于对用户的深度理解提供主动智能服务，如自动规划出行路线、推荐餐厅菜品等。

而在这幅手机厂商想布局长远的生态图里，隐私保护是这个故事的起点。

本报综合消息