买学习机却买来骚扰，谁在倒卖孩子信息

未成年人学情数据成灰色商品，一条能卖到三块钱

深壹度 SHEN YI DU

当孩子的错题记录、学习偏好、作息习惯，甚至细微的神情状态，都被悄然记录、归集、转手流转，一场潜藏在AI教育背后的未成年人隐私泄露乱象，正悄然浮出水面。

齐鲁晚报·齐鲁壹点记者调查发现，市面上很多智能学习硬件、线上编程课程等AI教育产品，早已化身24小时在线的隐秘数据采集终端。行业口中标榜的匿名脱敏、隐私保护机制落地形同虚设，漏洞随处可见，未成年人学情数据违规共享、无序外泄，已成为整个AI教育行业的共性隐患。

记者 郭春雨

市面上很多智能学习硬件、线上课程等AI教育产品，或许在你不经意间就收集了孩子的学情数据信息。

买学习机只为提分 却成“精准推销”目标

济南市民张女士的孩子读小学三年级，2025年她花近5000元购入一款主流品牌AI学习机。谁能想到，设备先变成了“精准推销”工具。一周后，孩子刚搜索“初中物理电学”，首页便弹出无法关闭的高价冲刺班广告；注册次日，张女士便接到自称“教务处”的电话，对方精准报出孩子的学科薄弱项，推荐一对一辅导。此后每周，她都会收到3到5条围绕孩子学习进度的营销短信，“精准得让人后背发凉”。

张女士翻查隐私权限发现，设备信息、使用记录、错题数据、学习时长、浏览轨迹，甚至位置信息、麦克风权限，全被平台默认开启。她重新翻阅隐私条款，发现其中有一句“同意向合作方提供匿名化学情数据，用于产品优化与商业推广”。“我以为去掉姓名、手机号就安全了，没想到平台能通过设备ID、学习行为直接锁定到具体家庭。”张女士说。

张女士的遭遇并非个例。记者梳理市面上主流教育AI产品发现，多家平台的隐私政策中都藏着类似的“授权共享”条款——用小字、专业术语堆砌，普通用户难以察觉。以“讯飞AI学”App为例：其隐私政策规定用户信息可在“关联公司”内共享，但“关联公司”模糊不清，用户如果拒绝，则无法使用相关程序。尤为值得关注的是，“讯飞AI学”提供的隐私政策仅描述“我们会共享/评估/要求第三方保护”的单方面自夸，却未提及用户有权拒绝共享。这无疑将用户推入默认同意的陷阱：用户打开App就默认勾选了所有SDK的共享。

此外，另外一款某主流学习机的用户隐私政策明确写道：“对于我们收集到的您的信息，我们将通过技术手段及时进行匿名化处理。在不泄露您个人信息的前提下，我们有权对匿名化处理后的用户数据进行分析、挖掘和利用，有权对智能产品的使用情况进行统计分析并用于可能的第三方信息共享。”

然而，数据工程师王磊告诉记者，所谓“匿名化数据”根本不是真正匿名，学情数据+设备ID+学习行为的组合，可精准锁定90%以上的用户家庭。“法律意义上的匿名化必须做到‘不可逆识别’，但多数平台仅处理姓名、手机号，却保留了设备ID、学习轨迹、学校年级等间接信息。“这些信息组合起来，足以精准锁定具体学生。”王磊举了个直观例子，“一台学习机的序列号，加上孩子‘每天19点做数学题、错题集中区域’的行为轨迹，再结合所在城市、年级，就能快速定位到具体家庭。”

权限设置层层壁垒 被动接受成唯一选择

比学习数据更隐蔽的，是对未成年人生物特征与行为轨迹的全方位捕捉。记者实测两款市面上主打的“AI智适应”学习机和学习App发现，即便关闭相机权限，前置摄像头仍会在做题过程中被后台调用，且应用界面无任何提示。当用贴纸遮住摄像头时，系统仅提示“专注力检测功能可能不可用”，核心学习功能并没有受到影响。两款设备测试下来，全程无弹窗告知“正在采集面部数据”。隐私协议仅笼统写着“为提升学习效果，可能会采集面部信息”，至于采集内容、去向及关闭方式均未明示。

值得注意的是，2025年工信部通报了20款存在侵害用户权益行为的智能终端产品，其中就包括某些品牌的学习终端。通报指出的问题之一是，部分智能终端在没有任何弹窗告知，甚至用户完全不知情的情况下，后台采集摄像头画面，并将生成的个人信息违规传输到云端。

“设备或者系统会实时标注学生‘专注度’‘微笑次数’‘低头频率’，这些数据会同步到学情数据库，作为推荐课程的重要依据。”王磊介绍，平台可以通过AI算法分析面部微表情，判断学生对知识点的接受程度，“比如皱眉次数过多，就判定为‘理解困难’，后续就可能定向推送高价辅导课”。

更令人担忧的是跨平台数据串联。记者发现，“讯飞AI学”“网易有道”“扇贝单词”“网易有道”“掌门1对1”“沪江网校”“Vipkid”“一起作业”等多款教育类App的隐私政策中，均包含与关联公司（或同一账号体系下的关联产品）共享用户个人信息的条款。这意味着：用户通过手机号注册其中某一款产品后，其账号信息、设备信息以及部分学习相关数据（具体类型因App而异），可能会依据隐私政策的约定，在运营方旗下的其他关联App之间进行共享。“相当于只要用同一个手机号登录过教育类App，你的所有学习行为都会被整合画像，形成完整的数据档案。”王磊表示，这种“数据互通”模式，让跨平台精准追踪成为可能。

这种“数据互通”让家长防不胜防。而想要拒绝这种采集，在技术上极难实现。不少教育平台隐私协议动辄上万字，涉及数据共享条款几十项，绝大多数家长根本看不懂，只能直接勾选“同意”。即便想关掉权限，也无处下手。记者实测发现，多款主流教育App首页根本找不到“一键关闭”入口，烦琐的多级菜单设置让非专业人士望而却步。更棘手的是，数据采集权限常与核心功能绑定——限制权限，孩子就无法正常上课。最终，家长只能用知情权换取设备的使用权。

学情数据明码标价 形成完整灰色产业链

学情数据的商业价值，远高于普通个人信息。曾深耕教培行业的张莉莉透露，通过学情数据能精准判断家庭消费能力、孩子的学习短板和焦虑点，定向广告转化率能达到35%以上，比普通广告效果好得多。

“普通的孩子姓名、电话，一条才卖5毛钱，但附带错题倾向、薄弱学科的精准学情信息，价格能翻一倍多，最高能卖到3块钱一条，还会在机构之间反复转卖。”张莉莉说，这种精准推销家长很难拒绝，“比如孩子刚考完数学，几何证明题失分多，机构马上就来推相关补课班，家长大多会动心。”

网络安全公司永信至诚的公开数据显示，2025年12月全球监测到约27.34亿条数据泄露记录，教育培训行业以17%的占比成为数据泄露风险最高的行业。这些泄露的数据，还成了“退费陷阱”等精准诈骗的工具。

司法判例则进一步揭开了数据泄露的具体路径和危害。2018年中国裁判文书网公布的判决书显示，司法判例揭示了数据泄露的严重性。2018年，科大讯飞员工张某利用维护学籍系统的权限，将数万条学生及家长信息以每条0.1元出售，非法获利约4000元，信息被多家教育机构用于电话招生并多次转卖。

如果说这起案件是“内部人员监守自盗”的单点漏洞，2025年四川宣判的一起案件，则暴露了一条从数据窃取到落地招生的完整灰色产业链，涉案学生信息达70余万条。案件的起因是凉山州冕宁县一位家长报案称，女儿信息泄露后，每天都接到大量招生、助考电话。警方调查后查明，信息泄露源头是四川某信息工程公司工程师彭某，该公司负责维护四川省教育资源公共服务平台，彭某利用权限接触到海量中小学生信息，通过外网群聊找到买家售卖。随后，这批数据在灰色链条中反复流转。整个链条上，涉案人员包括平台工作人员、中介、教育机构负责人，甚至学校副校长，目前相关人员均已获刑。

这些真实案例清晰表明，未成年人学情数据早已成了成本低、流通隐蔽、需求大的“灰色商品”。当本应记录学生成长的教育数据，变成了可随意买卖的“灰色货币”，平台所谓“优化服务”“提升体验”的合规说辞，显然难以掩盖商业利益对数据安全的侵蚀。

相关链接

整治学情数据违规交易 监管正持续发力

面对频发的学情数据泄露事件，不少家长追问：难道法律没有保护孩子的个人信息吗？

答案是否定的。北京市中闻律师事务所全国刑委会副主任、上海市人民检察院人民监督员张玉锋律师告诉记者，我国对未成年人信息的法律保护力度远高于成年人。《中华人民共和国个人信息保护法》第三十一条明确规定，处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。《儿童个人信息网络保护规定》第九条、第十条也要求，网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并征得同意，同时必须提供拒绝选项。在法律框架下，非法倒卖信息将面临严厉惩罚。出售公民个人信息达到法定数量即构成犯罪，涉事企业还可能面临吊销执照、行业禁入等处罚。

既然法律严明，学情数据的违规交易为何仍屡禁不止？在张玉锋看来，平台并非不知晓法律边界所在，而是在知情同意条款的设计、隐私收集的披露方式以及后续执行上，普遍利用了家长信息不对称的弱势——冗长的协议条款、层层嵌套的权限开关、与核心功能绑定的数据采集，使“知情同意”在实践中流于形式。

值得欣慰的是，学情数据灰色产业链带来的问题，正日益受到监管层面的高度关注。

2026年4月，中央网信办、工业和信息化部、公安部三部门联合发布公告，宣布将开展个人信息保护系列专项行动，教育领域被列为重点关注领域之一。公告明确提出，重点治理教育机构处理不满十四周岁未成年人个人信息未取得监护人同意、网站和App过度收集位置及学籍等敏感信息、校外培训机构向第三方提供个人信息未取得主体同意等问题。三部门明确表示，对情节严重、拒不整改的将依法从严处理。