“读取和写入”

你的人脸正飘在“云端”

从去年开始，人脸识别火遍大江南北，不少小区都以此为卖点，推出了人脸开门服务。但你有没有想过一个问题，你的人脸数据被采集后都去了哪里？

宁波某AI公司负责人L先生明确告诉记者：“有可能上云端了，而且你无法保证这些公司不把你的人脸数据泄露出去。”

他介绍，AI的原理是深度学习的神经网络，而如今有另一种技术叫“对抗神经网络”，也就是计算机可以通过泄露的人脸数据模拟出业主的人脸，从而解锁。

当然如果人脸数据泄露，那么一个人从哪里出来，去到哪里，理论上只要有摄像头都可以定位识别，因此人脸数据的保护规则也是亟待建立的。

那么，可能有读者要问了，公安系统也有人脸识别，是否安全呢？答案是肯定的。

L先生告诉记者，政务类大数据有明确的监管政策，需要达到中华人民共和国和公安部信息系统安全等级保护三级认证（简称“等保三级认证”）。此类数据库拥有专用的数据中心，单独的光纤传输，以及各类保障数据安全的技术和管理。

相比之下，市场中的互联网公司往往因成本因素没有建立完善的保护规则、防火墙，因此经常出现SaaS平台数据泄露的情况。

亲历大数据杀熟

大数据杀熟不是新闻了，携程、飞猪、艺龙在去年不停被媒体曝出大数据杀熟的新闻。记者去年在上海出差时亲历了一次。因为工作原因，记者去年出差的次数较多，一直使用携程订房。在入住上海浦东区金桥附近一家快捷酒店时，偶然间发现记者预定的房间所谓的“优惠折扣价”竟然比直接在前台开房还要贵出三分之一左右。

前台服务员也感到奇怪，用她的手机打开订房页面有5种房间价格，其中3种比前台价便宜，有两种较贵。而记者的订房页面只有两种较贵的价格。

其实这种技术最早出现在淘宝、京东等电商平台，就是根据顾客的购买力、偏爱在每个人打开APP浏览店铺时所显示个性化页面，也就是不同人浏览同一个店铺时所看到的商品不一样。2017年开始，如Zara、太平鸟、GXG等服装网店都启用了这种模式，当打开页面后，显示的是客户最新浏览过、搜索过，或加入购物车过的产品以及关联程度较高的商品。根据当时的数据使用“千人千面”后，服装网店的复购率（一位顾客第二次消费占所有消费顾客的比例）将由17%提高到近40%，不知不觉中就让你“剁手”。

但技术始终是把双刃剑，如果用技术干坏事，那么普通消费者将防不胜防。

怎么防范骚扰电话?

最后说一个消费者不胜其烦的老问题——骚扰电话。

近一年来，骚扰电话又有大举返潮的迹象。从工信部旗下的12321举报中心的数据看，它的最新报告显示，8月、9月共收到骚扰电话举报18万次，平均一个月9万次；而在 2018上半年，月均骚扰电话举报仅3万次左右。

为什么骚扰电话越来越多了？

第一个原因就是电销机器人的兴起，让骚扰更有效率了。

如果说以蒸汽机为标志的工业革命解放了人的体能，那么“电销机器人”可以称得上是电话销售行业的“蒸汽机”。

这种通过机器人拨打的销售电话，可以提前录制上百组的“定制话术”，判断你在通话时说出的语音，自动选择提前录制的录音，以自动播放的形式回复。

这样的电销机器人，每台价格三四千元，每天可以拨打800~1000个电话，相比以前呼叫中心每分钟0.1~0.15元的报价以及人工成本，效率更高的同时，成本也更低。这对饱受骚扰电话困扰的人来说，实在是个坏消息。

如果你也尝试用百度搜索电销机器人，就会发现这一个关键词命中了至少6条广告，可见现在的流行程度和竞争激烈。

那么，究竟怎么样降低骚扰电话对我们的侵扰呢？

中国移动宁波分公司市场部的技术专家介绍，目前移动公司已建立了一套完善的数据保护体系，包括“金库模式”(对涉及用户敏感信息的关键操作实现操作与授权分离)、4A等技术防护手段的应用和审计，提升客户信息保护能力，规范收集、存储、使用、销毁客户信息的行为，严控客户信息泄露风险。比如现在营业厅的客服人员，不允许查看到办理业务客户的完整信息，只能看到姓，不能看到名，手机号、身份证号也是隐去几位。同时，通过“事前”拦截、“事中”干预系统，为用户提供无感知的诈骗电话治理服务的同时，及时将线索推送公安机关；派驻专员进驻市反诈中心协助办案，累计拦截省内外诈骗呼叫5300万余次，协助公安破获案件780余起，为群众挽回损失近2000万元。

Z博士也提醒消费者在连接一些单次使用程序时，尽量少输入自己的手机号，如房产、汽车类互联网公司因经营原因，容易泄漏客户信息。

此外，中国移动宁波分公司市场部的技术专家也推荐了浙江移动一款新开发的防骚扰电话小程序，叫做“机伶”。这款程序会根据360等网站搜集的骚扰电话主叫方数据，在向外拨打电话时即切断，记者亲测有效，几乎可以屏蔽80%以上的骚扰电话。

责任编辑 诸新民 美编 徐哨 照排 张婧 校对 雷军虎