这里有一套互联网冲浪人必看的防身术!

3 为了追平台规划路线只能超速?

专家说

骑手追赶算法 算法被“训练”得越来越快

从去年的爆款文章《外卖骑手困在系统里》，到层出不穷的小哥危险驾驶事件，都足以说明，在算法的推动下，外卖骑手正在被迫变成配送机器，这份职业越来越危险。

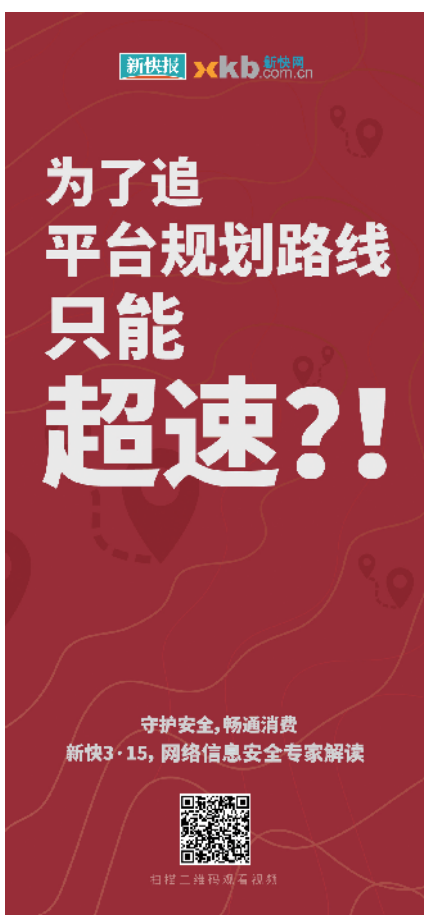
这是因为平台企业的竞争就是配送速度之争，它们纷纷推出各自的“人工智能配送算法”，时间是最重要的指标，超时哪怕只有一分钟，骑手也会面临差评、罚款。

算法帮骑手规划好多个订单的取送餐顺序，并为每一单提供路线导航，算法要求骑手越跑越快，而骑手们在超时的惩戒面前，也会尽量去满足算法的要求。这样的配送行为也变相把越来越多的“短时长数据”给予算法。数据是算法的基础，它会去训练算法，当算法发现原来大家都越来越快，它也会再次加速，倒逼骑手铤而走险。

To 企业

让更多相关方参与制定算法 精准缩小商家配送范围

一是考虑让更多的人参与到人工智能算法规则的制定和协商中。外卖经济的网络组成部分非常多元。除了平台和消费者，还有店家、中介公司、骑手等。当算法嵌入到社会生活的方方面面时，就不是单一的“平台–消费者”关系。算法的制定者不仅来自平台高管和程序员，还包括骑手、科学家、第三方机构、政府等。二是改进算法。随着数据积累得越来越多，算法可以更精准缩小一些商家的配送范围，让骑手配送距离更近的订单，规划路线更为合理。



4 手机App会偷走你的照片和通话记录?

专家说

绝大部分App只需10个(含)以下与个人信息相关的权限

手机App通过获取写入及读取外置存储器、读取电话状态（设备IMSI/IMEI号）、拍摄、访问粗略定位、访问精准定位、录音、读取通讯录、拨打电话等权限，能够读到的信息有：短信/彩信、照片、通话记录、通信录、日历、已安装应用列表、身体传感器信息等。

这样一来，就会导致存在个人信息违规收集和恶意滥用风险，不少App都要求消费者授权所有权限，没有遵循最小够用原则。实际上，绝大部分App申请10个(含)以下与个人信息相关的权限即可满足需要。有些App私自共享用户数据，就是未经用户同意与第三方共享个人信息。有些App过度留存个人数据，普遍存在“注册容易注销难”的现象，注销用户设置限制条件多，甚至不提供注销功能。

To 企业

积极开展安全评估 公示预置应用软件相关信息

一是App运营者应落实数据安全主体责任，建立企业内部的数据安全与个人信息保护机制，积极定期开展数据安全与个人信息保护第三方评估或自评估工作。二是应用商店等平台应加强应用上架前数据安全审核，将数据安全与个人信息保护措施作为重点审核内容，对违法违规App不予上架。三是移动智能终端企业应严格落实应用软件预置管理要求，并向消费者公示预置应用软件相关信息，重点明示应用软件安装及运行所需权限列表，收集、使用用户个人信息的内容、目的、方式和范围等，拒绝与不符合规范要求的软件提供商合作。

To 监管方

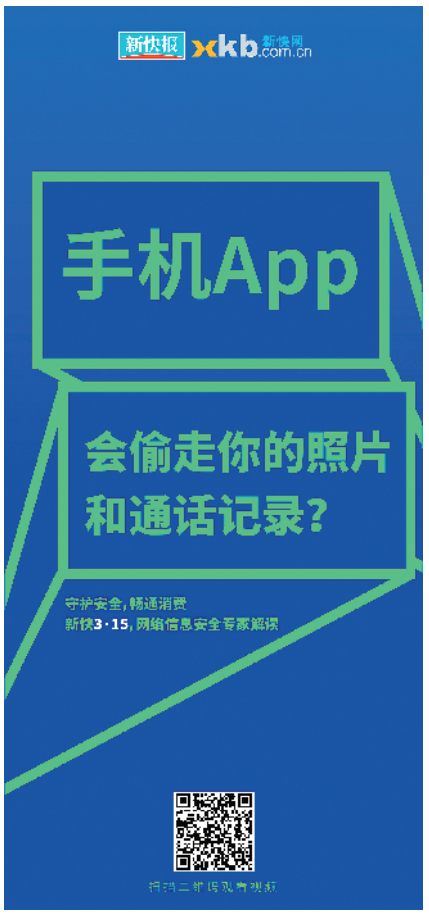
出台技术规范标准 指导企业加大安全投入

一是继续推进App个人信息专项整治行动。把违规的App下架、约谈企业，是一个很好的监管手段。二是加大消费者宣传教育力度，App数量保守算有350万个以上，数量非常庞大，监管的难度很大，需要消费者积极参与。三是应推动行业提升App数据安全与个人信息保护技术水平，出台相关技术标准规范，指导企业加大数据安全技术投入，提升企业数据安全保障能力。四是应加大工业互联网、工业软件新业态新领域的个人信息保护力度，打好信息安全基础，保障新业态新领域健康发展。

To 消费者

功能不用及时关闭 不要怕麻烦就给予多余的授权

一是要在各大正规应用商城安装应用，同类应用要选择安装平台认证过的或者下载量较多的应用，从源头上避免安装山寨的、带勒索病毒等的应用。二是授予敏感权限应谨慎，下载安装App时认真阅读权限提醒，谨慎开启权限，需关注相关权限是否为使用该应用所必需的权限，特别是录音、读取通讯录、访问位置等较容易直接泄露个人敏感信息的权限，这些权限最好也不要同意授权。三是使用应用特定功能时再打开相关权限，不使用时及时关闭。四是对于不影响应用使用的权限，拒绝申请并点击“不再询问”。有些应用经常频繁申请获取用户敏感权限，消费者往往不堪其扰而点同意，但这些常常是非必要权限，不要因为麻烦而给予多余的授权。



5 智能汽车联网后黑客帮你开?

专家说

4个轮子的“大手机”被黑 可能会车毁人亡

随着汽车智能化、网联化和电动化程度的不断提高，未来的汽车不再是简单的出行工具，而是融入消费者日常生活的多场景智能体验终端，可以视为带4个轮子的“大手机”。尽管当前智能网联汽车的安全漏洞尚未被广泛利用，但是不少的消费者表示信息安全和隐私保护将成为他们购买车辆时主要考虑的因素。

如果没有做好安全防护，就会出现影响汽车正常运行、车辆被非法锁定和控制、云平台被攻破等情况，造成个人隐私泄露、企业经济损失，还能造成车毁人亡的严重后果，甚至上升成为国家公共安全问题。

To 企业

敏感数据单独储存 通过加密提升安全性

信息安全是系统工程，一是需要把信息安全融入车辆研发、生产、测试、安全响应等整个生命周期，落实“最小特权”“纵深防御”等原则，不能“先上车再补票”；二是要重视车联网服务平台的安全防护，车联网服务平台是重要信息系统，按照网络安全法要求，定期进行网络安全等级保护测评；三是要做好数据分级管理，加强敏感信息管理，对于涉及消费者信息、驾驶习惯、车辆信息、位置信息等敏感数据采取较高级别的管理要求，仅被整车厂商签名认证的应用才可读取相关数据，其他非签名认证应用仅可读取非敏感数据。针对敏感数据实行单独的存储要求，通过加密提升数据安全级别。

To 监管方

出台相关完善技术标准 信息安全防护体系强制纳入生产

一是加强智能汽车在使用过程中数据采集的监管，加快出台数据安全以及个人信息保护等相关法规，并在汽车行业细化实施，禁止采集消费者非授权数据。二是技术标准有待进一步完善，虽然我国已经发布了一些标准（如车载信息安全技术要求和网联汽车信息安全技术要求两项团体标准），还缺乏较为完善的系列标准，相关的安全测试方法仍在研究中。三是要进一步鼓励和引导汽车生产企业，将智能汽车的信息安全防护体系纳入车辆生产、销售和服务的各个环节中，并形成强制性要求。

To 消费者

保护好交互最多的手机 网联汽车软件固件及时更新

一是要关注车企对自身产品信息安全的投入，如取得了什么样的信息安全认证，数据安全方面做了哪些工作？二是保护好个人的智能手机，智能手机和智能汽车交互比较多，黑客会通过root用户的手机或者诱导用户下载安装恶意应用，就可以窃取用户个人信息及车辆的控制权。三是要及时对网联汽车软件和固件更新，给安全漏洞打上补丁，这样能够最大限度避免安全风险。