

想要“更懂我” 担心“太懂我”

APP 的爱与恨:过度获取权限屡禁不止



最近,关于外卖 APP 可能“偷听”用户的猜测引起许多关注和讨论。相关企业很快否认,强调“监听用户日常对话并做信息分析”是一种无端猜测,并没有相应产品设置。虽然如此,但此类讨论依然显示出大多数用户对 APP 等网络应用的爱与恨:既希望更便捷、“更懂我”,又担心了解太多隐私信息,以至于“太懂我”。

对于这类问题,我国从 2017 年开始施行的《网络安全法》确立了网络运营者收集、使用个人信息必须遵循合法、正当、必要等原则。但随着用户个人信息被搜集、存储的机会越来越多,各类侵犯用户隐私信息的行为依然层出不穷,一些涉隐私的用户数据泄露事件也频频发生,APP 过度索取权限、超范围收集、使用个人信息等现象屡禁不止。

针对这类现实问题,前不久闭幕的全国两会也传出消息,《个人信息保护法》已被提上本届全国人大立法日程。3月15日,国家市场监督管理总局、中央网信办也联合发布了《关于开展 APP 安全认证工作的公告》及实施规则,以规范 APP 收集、使用用户信息特别是个人信息的行为,加强个人信息安全保护。

不过,记者采访后了解到,这些监管政策在促进隐私保护体系日趋完善的同时,也面临着不小的阻力。各方也在寻找,除法律法规等力量以外,还有哪些市场和技术力量可以平衡隐私保护与数据效率这对矛盾?

屡禁不止 近七成用户遭遇 APP 过度获取隐私权限

在搜索引擎中查看了大量关于雅思考试的内容后,武汉大学学生林海手机中的购物 APP 首页就被雅思相关书籍和材料攻陷了。“开始是惊讶,随后是愤怒,然后又感到害怕。”他这样形容自己发现这一事实后的感受。

在当下,此类现象屡见不鲜。另一位大学生杨小叶在手机上安装了一款镜子 APP,在无意间,她发现这个 APP 竟然“合法”地访问了她的通讯录。另一款功能单一的手电筒 APP 甚至冠冕堂皇地要求获得手机的录音权限。

2018年7月17日至8月13日,中国消费者协会组织开展的“APP 个人信息泄露情况”问卷调查显示,85.2%的受访者表示遭遇过 APP 个人信息泄露情况;67.2%的受访者表示,自己所使用的 APP 在其功能不

必要的情况下获取了手机中的隐私权限。

这项调查还显示,读取位置信息权限和访问联系人权限,是安装和使用手机 APP 时遇到最多的情况,通话记录、短信记录、摄像头、话筒录音等权限也常常被 APP 要求获取。

中国政法大学传播法研究中心副主任朱巍对 APP 过度获取隐私权限的行为深有体会。他曾在手机上安装使用过一个著名 APP,但因为经常发送广告,他就把这个 APP 卸载了。但卸载之后,他还是能时不时地收到该 APP 平台发来的短信广告,有时甚至还会根据他所在的城市推送相应的广告。朱巍猜测,这可能是因为在开始使用这个 APP 时,就在使用协议中允许其获取过多的隐私权限。

观韬中茂(上海)律师事务所合伙人王

渝伟认为,由于许多企业积弊难改,自身合法合规和政府执法都需要时间和经济成本,再加上过度收集信息所获取的经济收益诱人,这些因素都致使相关法律法规的推行困难。

腾讯公司法务部数据及隐私中心负责人黄晓林指出,APP 获取用户权限过多、过度的问题由来已久,有些 APP 超出必要范围获取用户的敏感权限很不应该。但这些现象屡禁不止的原因在于,其所面临的法律风险可能远远小于可以获得的商业利益。

黄晓林还补充说,有很多 APP 集成了多种功能,甚至在未来的迭代升级中会具备更多功能,为了实现这些功能,APP 会要求获取更多权限。在这种情况下,判断其是否过度获取用户权限,是否合规,还需要针对每个 APP 的具体功能来做具体判断。

制定规范 APP 安全认证开始实施

针对 APP 过度获取隐私权限等现象,3月15日“国际消费者权益日”当天,国家市场监督管理总局和中央网信办联合出台了《关于 APP 安全认证的公告》,指定中国网络安全审查技术与认证中心(ISCCC)为官方认证机构,依据《信息安全技术个人信息安全规范》来制定技术验证规范,对 APP 进行安全认证。

记者了解到,上述 APP 安全认证相关通道已于 3 月 21 日正式开通。认证秉承自愿原则,按照“技术验证+现场核查+获证后监督”的模式进行,对于通过认证的 APP,将鼓励搜索平台和应用商店优先推荐。针对 APP 中涉及个人信息安全的具体技术验证规范已经制定完成,将会对参与验证的机构公开。

作为互联网公司的隐私保护从业者,黄晓林对上述 APP 认证持相对乐观的态度,“对整个行业,对个体和隐私保护(这方面),都会有更加正向的作用,会引领各家企业更加重视这方面的内容。”

黄晓林也指出,目前市场上 APP 数量众多,企业能否花费足够的时间和经济成本参与其中还有待观察。但对占据大多数市场份额的 APP 和企业来说,这是一种自我纠错的过程,可能从源头上推动企业更加合规。他期待,这类 APP 安全认证工作可以在更多技术手段的帮助下,更加自动化、高效率,甚至像杀毒软件一样普及,从而进一步推动 APP 合规运营。

作为长期关注隐私保护领域的律师,王渝伟表示,APP 安全认证的做法属于市场调

节的治理方法,将使得隐私治理的手段更加多样化。不过他也指出,尽管此次 APP 安全认证的框架已定,但是仍存在许多边界不够明确的地方。例如,细则中出现了重大信息安全事件这一概念,但现行法律对于如何界定重大信息安全事件尚无明确规定。

中国网络安全审查技术与认证中心(ISCCC)相关人员告诉记者,目前尚无对上述概念的明确定义,将会参照部分个人信息安全相关的评估指南来作为评判的标准。从公开的细则来看,目前对于通过认证的 APP 主要的监管手段依然是以企业自查为主,辅之以社会监督,但真正交由第三方的监督却十分有限。同时,由于认证是自愿进行,未通过认证的 APP 如何管理依然没有得到彻底有效的解决。

鼓励制衡 技术界寻找解决方案

对于因大数据技术的发展而带来的隐私保护问题,技术界也在关注并且研究相应的解决办法。

3月23日,在中国计算机学会青年计算机科技论坛(CCF YOCSEF)举办的“人工智能时代,隐私和效率一定是不可调和的吗?”专题讨论中,有技术人员介绍称,在杭州等地已经在尝试基于区块链技术开展隐私保护,大致的思路是利用公有链形式开展数据交易,以联盟链形式开展数据加密保护。

对于区块链技术在隐私保护领域的应用,中国人民大学教授孟小峰指出,去中心化、可溯源的区块链技术是一个可以研究

的隐私保护方向,其有利于在隐私泄露之后溯源、追责,但由于技术尚不成熟,效率不高等问题,区块链技术应用于隐私保护领域还处于探索阶段,而且区块链的使用成本也较高,监管部门或者企业会否采用尚无法确定。

作为技术界的实践者,360 行业安全研究中心主任裴志勇认为,采用区块链或是大数据技术来监测隐私泄露情况在技术上都是可行的,但是在实际操作中则面临着成本过高和依然需要大量人力资源的问题。

在上述专题讨论会议上,裴志勇提出一个设想,将目前应用于云计算领域的“三

方制衡原则”引入到 APP 安全监管中:将涉隐私的个人数据所有者、运营者和管理者相分离,避免一个主体既是裁判又是运动员,把这种制衡的能力商业化,鼓励一种能够制衡企业利用用户数据的产业快速发展,从而形成长期持续的市场化监管。

作为法律学者,朱巍认可裴志勇提出的上述观点。“不能一个人又当运动员,又当裁判,政府不行,企业也不行。”他认为,即将出台的个人信息保护法需要作出底线规定,让个人信息保护真正回归到个人权利本身,在此基础上,通过企业之间的相互竞争与制衡,寻找更多更可行的办法。

(王林 孙吉)