

69款移动应用过度收集使用个人信息被通报 应用程序岂能变身“隐私刺客”？

这69款移动应用 违规被通报

近日,据国家网络与信息安全信息通报中心通报,依据《网络安全法》《个人信息保护法》等法律法规,按照《中央网信办、工业和信息化部、公安部、市场监管总局关于开展2025年个人信息保护系列专项行动的公告》要求,经国家计算机病毒应急处理中心检测,69款移动应用存在违法违规收集使用个人信息情况。

其中,15款移动应用在App首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则;隐私政策难以访问;个人信息处理者在处理个人信息前,未以显著方式、清晰易懂的语言真实、准确、完整地个人告知个人信息处理者的名称或者姓名、联系方式、个人信息的保存期限等。

39款移动应用的隐私政策未逐一列出App,包括委托的第三方或嵌入的第三方代码、插件,收集使用个人信息的目的、方式、范围等。

15款移动应用在个人信息处理者向其他个人信息处理者提供其处理的个人信息的,未向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类,并取得个人的单独同意。

3款移动应用未在征得用户同意后才开始收集个人信息或打开可收集个人信息的权限。

8款移动应用未提供有效的更正、删除个人信息及注销用户账号功能;为更正、删除个人信息或注销用户账号设置不必要或不合理条件;虽提供了更正、删除个人信息及注销用户账号功能,但未及时响应用户相应操作,需人工处理的,未在承诺时限内完成核查和处理。

3款移动应用的投诉、举报未在承诺时限内受理并处理;个人信息处理者未建立便捷的个人信息权利的受理和处理机制。

35款移动应用未向用户提供撤回同意收集个人信息的途径、方式;个人信息处理者未提供便捷的撤回同意的方式。

作为普通用户 如何防范隐私刺客

作为普通用户,如何防范隐私刺客呢?业内人士给出一些方法。

方法一:不再使用的应用程序,应及时注销账户并删除个人资料。

北京市互联网信息办公室网络安全协调处工作人员孟翔介绍,我们在生活中使用一些小程序或者App的时候可能会暂时使用,或者这段时间使用完以后,后面就不再使用了,从安全的角度,就应该删除里边存储的个人信息。具有个人信息收集这种功能的小程序,都应该提供账户的注销,或者说个人信息删除、更改这种功能,如果没有提供的话,理论上应该就属于违规行为。

依据《网络数据安全管



例》第二十四条规定,个人注销账号的,网络数据处理者应当删除个人信息或者进行匿名化处理。删除、匿名化处理个人信息从技术上难以实现的,网络数据处理者应当停止除存储和采取必要的安全保护措施之外的处理。

方法二:定期检查App权限设置,及时关闭非必要授权。

北京理工大学法学院教授洪延青介绍,现在很多手机操作系统提供了这样的一个机制,比如在打开某些地图软件的时候,或者打开某些点餐软件的时候,它会提示你的麦克风的权限被打开了,也许这个场景里你没有使用麦克风,就可以到后台去查看是否过多地授予权限,你完全可以自主地防范它。

方法三:对频繁索权、诱导授权的应用,坚决拒绝安装。

孟翔介绍,比如说这个软件没有必要收集我们的位置信息,它的基础的业务功能不需要位置信息,但是它一次两次三次反复向我们弹窗索要位置信息的权限,我们拒绝,但是它仍然反复提醒,这种也属于违规行为。

方法四:关注违规App名单,防患于未然。

洪延青介绍,其实全国各地都在开展自己辖区内的专项整治活动,我们可以关注这些执法部门定期发布的公告。如果看到公告里出现的已经违法违规收集处理个人信息的App,用户就可以少下载或者不下载这类App。

方法五:发现违规收集个人信息行为,积极举报。

北京市互联网信息办公室网络安全协调处处长杨虎提醒广大用户,可以通过12345市民服务热线进行投诉举报,他们将依法依规地予以处置。下一步他们也将按照中央网信办、公安部、工信部、市场监管总局关于2025年个人信息保护的专项行动的安排,会同有关部门深入开展民生消费领域违法违规收集个人信息问题的专项治理,维护广大用户权益。

不能仅靠“点名通报” 应让违规者付出代价

《个人信息保护法》明确规定,处理个人信息应当遵循合法、正当、必要和诚信原则,应当取得个人的单独同意。然而在现实中,“知情同意”却成了极易被突破的防线。有的App信息授权协议“含糊其词”,用户对会收集哪些信息迷惑不解;更有甚者,“默认同意”“强买强卖”,直接剥夺了用户的选择权;也有一些用户对隐私政策并不关心,因为文本太长就“盲点同意”。不少看似便捷的App,利用“隐蔽手段”成了潜伏在我们身边的“隐私刺客”。

面对“隐私刺客”,仅靠“点名通报”恐怕难以形成足够威慑,必须让违规者付出代价:该重罚的绝不手软,该下架的果断下架。唯有如此,相关企业才能打消“以身试法”的冲动。

对用户而言,也要从“被动接受”转向“主动保护”,谨慎授权App获取个人信息,定期检查个人信息的使用情况,对于不再使用的App要及时注销账户信息。

保护个人信息是一场持久战。这需要监管部门建立常态化监管,探索引入第三方专业机构对App隐私政策等进行监督,斩断各类黑产背后的黑手,建立全链条、可追溯的责任体系。需要企业与平台及时排查安全隐患,提高技术防线,堵上系统漏洞,以事前预防取代事后补救,将个人信息保护内化为产品“基因”。还需要用户不断增长新媒体素养,敢于对侵权行为说“不”。

用户信任是最宝贵的资产,漠视用户隐私的企业,终将被市场抛弃。把“隐私刺客”关进笼子里,真正用好大数据,将依法依规掌握的消费者信息应用在改进产品与服务上,在良性互动中实现互利共赢,才是数字时代企业与平台的长远发展之道。

据央视新闻、人民日报

“刚开学就下载了快10个App!平时通知在微信,线上签到要在学习通、U校园上完成,有时候老师让签到,我都搞不清在哪个平台。”四川一高校大一新生王欣(化名)看着手机里密密麻麻的图标,忍不住吐槽。这些校园App本应让学生学习更便捷,可“麻烦”“有负担”“很烦躁”,却成了大学生对它们的普遍感受。



记者 巩悦悦
实习生 白应婵 蹇悦 报道

App扎堆下载 功能重叠还占内存

“用过10个左右的App,像企业微信、学习通,知到、U校园这些都有。”深圳一高校学生小童(化名)介绍,“豆包用来解题,学习通和知到来签到,咕咚跑专门打卡校园跑。”

王欣回忆,这些App都是开学时老师要求下载的。“当时就觉得平台太多,怕后面用的时候弄混。”她无奈地说,很多App功能高度重叠,大多和线上课相关,都是看视频,却非要一个个单独下载。

更让人头疼的是切换麻烦。“学习通和知到能签到、交作业,可老师要求不一样,得来回切换。”小童说,切换时要退出当前课程页找图标,不同App的作业入口、测试界面差别大,还得重新适应操作逻辑。

王欣还提到,有些课程完全能在一个App上搞定,却被拆到好几个平台。“比如英语课,通知在微信,签到看视频在U校园,考试又用专门的考试App,做任务还可能换另一个。”原本简单的事,变得“环节太多,太麻烦”。

还有不少App下载后使用率极低。“有的App里有校园社交、付费考证课、直播带货这些功能,我从来没用过。”王欣说,还有个混合教学App,下载后只用过一次,但也不敢删,“太占手机内存了”。

高频使用却体验差 槽点一箩筐

“这些App使用频率特别高,上课签到、做作业都得用。”王欣说,可体验感实在一般,“App里总弹广告,关闭按钮藏在角落,就一个小小的‘跳过’,稍微不注意就误触。”

小童也遇到过不少问题:“期末高峰时段网课卡顿,提交大文件作业加载半天,论文查

重辅助功能还偶尔闪退。”

王欣对学校的洗澡App吐槽最多:“每次洗澡都得用它刷卡,进去就弹广告,特别容易点错。而且不管账户里有没有钱,都会突然断水,得重新打开App启动热水器,太折腾了。”她还说,这个App还总强制更新,“一周能更两三次,有时候着急洗澡,舍友们都等着用,更新半天特别耽误时间。”

信息泄露风险也让学生担忧。“校园跑App必须开定位,不然记不了步数,还总显示没信号,让我同时开WiFi和流量。”王欣直言,对这种强制授权的App,总担心个人信息会泄露。

有些高校 已着手优化

面对这些问题,学生们的诉求很明确:“相同功能的App可以合并一部分,尤其是老师要求下载的,其实核心功能就那几个,选两三个够用就行。”王欣说。

小童更希望能整合到一个平台:“减少切换的麻烦,避免功能重复,把专业课笔记、作业、网课进度集中管理,实现数据互通,学习效率也能提高。”他还建议,先合并网课播放、课件下载、真题刷题、电子笔记、作业提交这些核心功能,同时保留课程适配精准、运行稳定、数据自动备份的优势。

功能上,学生们还有更多期待:“希望加智能错题分类、论文参考文献自动排版、学习进度可视化,最好能根据期末考点推送习题。”

针对广告多、更新频繁的问题,学生们也盼着改善。“应该减少更新频率,没实质功能变化就别更了。”王欣说,广告植入也得减一减,别总让人分心。

记者了解到,有些高校开始听取学生建议,优化平台服务。“我们收到了学生反馈,说有些业务处理流程太繁琐。”山东一高校辅导员孙老师说,“我们会及时反馈给数字化办公室,他们会根据意见简化流程。”

“去年下半年,我们已经把所有工作整合到一个App平台上了。”孙老师表示,整合后确实方便了不少,“下一步希望能更简单明晰,让学生操作起来少点复杂步骤。”

刚开学就下载了快十个,本意『便捷』实则『麻烦』
校园App功能重叠广告多,『瘦身』呼声高