

信息安全风险怎么破？

随着互联网

生活在人们的日常生活中占比越来越大,很多生活和消费场景都从线下转移到线上,如何安全地享受网络带来的便捷和红利,如何在冲浪的同时维护自身的财产和隐私,互联网信息安全是一个大家越来越关注的话题。

据广州市消委会召开的 2021 年“3·15”信息通报会上公布的数据显示,互联网服务类的投诉量排行位列前五。借 3·15 的契机,新快报携手工业和信息化部电子第五研究所信息安全中心,选出网络热议的五大典型信息安全风险场景,请专家分析现象发生的来龙去脉,用通俗易懂的语言科普解惑,给监管方和企业提整改建议意见,教消费者如何防范。

■策划:新快报记者 罗韵
■统筹:新快报记者 梁或
■采写:新快报记者 罗韵
■视频制作:陈文锋 莫根源 陈宝贤 蔡佳
■美术:蔡鸣帆
■制图:廖木兴

1

售楼部买房看脸给价格？

专家说

人脸信息被采集“等于把自家钥匙公之于众”

客户戴着头盔去售楼部看房的视频,引起了网友的热议。工业和信息化部电子第五研究所信息安全中心高级工程师刘锐奇告诉新快报记者,在业内第一次上门由中介带看的渠道客户,能拿到售楼部承诺给中介的优惠价格。自己来的客户称之为散客。在售楼部看来,散客不应当享受跟“渠道客户”一样的优惠。

为了区别客源,就采用了人脸识别系统,用来精准捕捉信息,“看脸”给价格。

“作为身份验证手段,人脸识别技术存在先天缺陷。相对于指纹、虹膜、基因等的生物特征信息,人脸暴露度较高,更容易实现被动采集(无感支付),这也同时意味着人脸信息更容易被窃取。特别是人脸信息具有唯一性,一旦丢失就是

等于把自己家的‘钥匙’公之于众,后果不堪设想,不仅可能侵犯个人隐私,还会带来财产损失。而大规模的人脸数据库泄露还会对一个族群或国家带来安全风险。”

To 企业

通过第三方检测确认安全性 对数据选择“即时储存”

第一,采集人脸数据前须告知用途和可能风险,在采集位置应该设有标志告知消费者,以保障公众知情权与选择权,防止企业过度收集和利用。第二,对人脸数据做好安全管理,确保数据在采集、传输、使用和存储过程中的安全性,可通过第三方检测认证或自评估的方式,确认企业是否具有相应技术能力保

障人脸数据的安全性。第三,根据数据用途,明确规定人脸数据的存储主体、时限和采集,依据人脸数据的使用目的和需要,可将数据的存储时限分为即时、短期和长期三类,并尽可能选择即时存储方式,即比对后不对扫描到的人脸数据进行保存,数据只是在“缓存”里临时保存。

To 监管方

完善法律法规 明确主体责任和不同场景应用的规范

首先,需尽快完善包括人脸识别在内的人体生物信息使用法律法规,在个人信息保护规范的基础上采取更严格的保护措施,明确生物识别技术可用场景、收集信息主

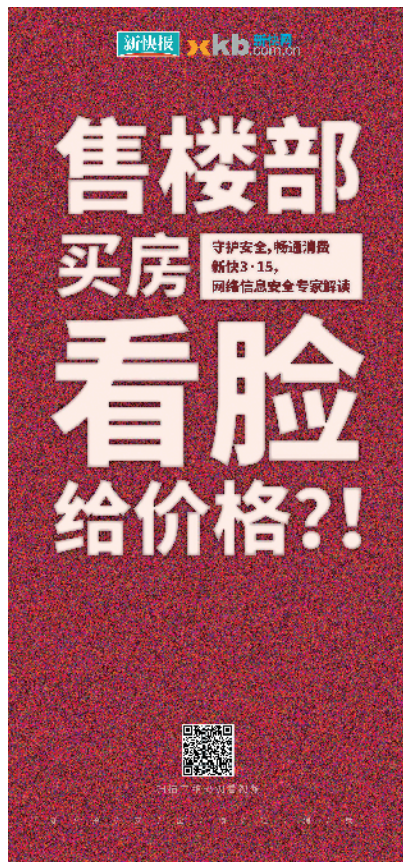
体应承担的责任和义务。其次是通过标准体系明确不同场景下的应用规范。应针对不同的应用场景设置不同的监管要求,并规定人脸信息收集、存储、处理等使用要求。

To 消费者

App隐私条款要读 可疑应用采集信息要拒绝

当前,各种采集人脸数据的产品和应用层出不穷,个人在面临各种信息采集的同时,必须要增强自我隐私保护意识,留

意公共场所采集人脸数据的标志,认真阅读相关隐私条款,个人手机上有可疑的应用,应当明确拒绝其人脸信息收集行为。



2

贵手机打车订酒店价格更高？

专家说

“大数据杀熟”就是利用隐私信息分析消费者心理价位

“大数据杀熟”的具体表现,就是同一件商品或者服务,互联网厂商显示给老用户的价要高于新用户。本质上是经营者为了获得最大利润,利用消费者的消费信息,分析消费者最低心理价位,对消费者进行分类,进行差异化定价的行为。最简

单的分类方法就是把用户分为价格敏感的用户和非价格敏感的用户,由于使用习惯老客户多为非价格敏感的用户,而新用户则对价格比较敏感。这里的“新用户”不仅仅是指新注册的用户,更多的是指停止使用一段时间后又回归的用户。

To 企业

产品开发阶段就要“系上数据安全的安全带”

应坚持“以消费者为核心”的思维,用更多优质服务吸引用户和增加用户黏性,而不是通过“大数据杀熟”的方式谋

求短期利益;在对大数据进行商业开发时,系好数据安全的“安全带”,不能触碰法律和道德底线。

To 监管方

完善取证技术和申诉方式

一是要完善“大数据杀熟”取证技术和程序,由于信息不对称,在复杂的优惠规则和相对私密的支付过程下,“杀熟”具有较强隐蔽性不易被发现,所以要想办法解决发现难、举证难、认定难的问题。二是

监管部门需大力推进商品和服务信息公开透明,打破信息不对称,让消费者有完整的知情权,能够在透明的情况下做出消费决策;三是要完善用户的申诉方式,为申诉提供更便利的途径。

To 消费者

遇到价格歧视用手机截屏或录视频

一是注意自己的隐私保护,尽量不让自身信息在社交网站、手机 App 等暴露得太多,尽可能地不要让地理位置、通讯录、相册等隐私被获取。二是当遇到疑

似“大数据杀熟”时,可以“货比三家”。如发现确实存在价格歧视,应通过手机截屏或是录制视频等方式留存证据,并向市场监督管理部门反映。

