

【新闻与传播】

我国移动 APP 隐私保护政策研究

——基于 96 个移动应用 APP 的分析

朱 颖

(广东外语外贸大学 新闻与传播学院, 广东 广州 510006)

【摘 要】 透过我国 11 类共 96 个移动互联网客户端 APP 隐私保护政策的一般情况和具体内容分析,发现我国移动 APP 在隐私保护政策制定和实施方面的问题主要有:水平参差不齐、存在霸王条款、缺乏协商机制、效果不够理想。要实现我国移动 APP 隐私保护政策的良好效果,应该加强政府监督管理、设置行业自律组织、促进企业内部自律、增强网民隐私意识。

【关键词】 移动 APP; 隐私保护政策; 行业自律; 法律规制

【中图分类号】 G206 【文献标识码】 A 【文章编号】 1000-5072(2017)12-0107-08

一、研究缘起

随着新媒体技术的发展,移动互联网日益渗透到人们的学习、工作和生活中。根据中国互联网络信息中心(CNNIC)在京发布的第 40 次《中国互联网络发展状况统计报告》指出:“截至 2017 年 6 月,中国网民规模达 7.51 亿,互联网普及率达到 54.3%……我国手机网民规模达 7.24 亿,有 96.3% 的网民通过手机上网,手机上网比例持续提升。”2017 年 8 月,工信部发布 2017 年上半年我国互联网业务运行情况报告,我国移动应用程序(APP)市场持续活跃,数量已超 402 万款。^①

现如今,人们越来越依赖手机、平板等移动设备交流、学习和生活,通过移动客户端 APP 传输和记录的数据也越来越多,移动 APP 的高频使用和大量信息的交换与传播使得隐私安全事故发生的风险不断扩大。据《2015 年安卓 APP 安全漏洞分析报告》分析:“2015 年,移动客户端 APP 安全事件泄露的信息以用户的姓名、地址、账号、密码、手机号等信息为主,其中金融理财和生活服务类 APP 是安全事件爆发的重灾区……2015 年超过 10 家知名 APP 被爆存在安全漏洞,可导致 1 000 万用户隐私泄露。”^②《2016 年度中国移动 APP 安全监测报告》则指出,2016 年度“信息和数据泄露事件屡见不鲜,如雅虎 10 亿信息泄露、1.17 亿 LinkedIn 账户登录信息泄露”^③。此外,个人信息数据

【收稿日期】 2017-09-01

【作者简介】 朱 颖(1978—),女,江西萍乡人,广东外语外贸大学新闻与传播学院教授,新闻学博士,主要从事新闻传播法制与伦理、政治传播研究。

【基金项目】 教育部哲学社会科学重大攻关项目“国家语言文字事业法律法规体系健全与完善研究”(批准号:14JZD050);国家社科基金重大项目“互联网与表达权的法律边界研究”(批准号:15ZDB144)。

① 姚翀《我国手机 APP 应用数量已超过 402 万款,游戏生活类应用“称霸”市场》,《南方日报》2017 年 8 月 10 日,第 B02 版。

② 《2015 年安卓 APP 安全漏洞分析报告》,Web 开发网,http://www.cncms.com/2016/0301/13920.shtml,2016-03-01。

③ 《2016 年度中国移动 APP 安全监测报告》,通付盾官网,https://www.tongfudun.com/industrytrend/243.jhtml,2017-01-03。

已经被明码标价进行买卖。比如 AT&T 公司以每月 20 美元向用户(subscriber) 购买“上网偏好”, 这些信息包括个人浏览数据; 又如 Datacoup 公司, 每月向用户购买他们在 Facebook 上的活动数据和信用卡使用情况。^①

移动互联网隐私保护问题日益为国际所重视。在移动 APP 的隐私保护安全链中, 隐私保护政策成为重要的一环, 主要是互联网企业制定用户隐私保护条款, 告知用户网站将如何采集、使用和保护用户的个人信息安全, 及其个人对数据享有的权利。隐私保护政策可以提高用户的信任, 缓解用户的隐私担忧, 既是网站保护用户的自律措施, 也是用户法律维权的重要保障。本文通过对多个移动 APP 隐私保护政策的实证研究, 考察移动 APP 隐私保护政策的内容是否全面、规定是否合理、手段是否有效, 无论对于 APP 经营者还是我国有关管理部门, 都能提供经验参考。

二、文献回顾

新媒体时代, 隐私权的内涵和外延都有所变化。自 1890 年塞缪尔·沃伦和路易斯·布兰代斯提出隐私权的概念, 认为隐私权是“保护个人生活不受干扰、独处的权利, 即个人具有不可侵害的人格, 对其思想、情绪和感受等自身事务的公开、揭露具有决定的权利”^②以来, 传统对于隐私权概念主要侧重于保护精神性人格权益。由于社会经济的发展, 信息社会的形成, 隐私权的范围更扩大至个人对其数据的控制。正如有学者(王泽鉴, 2009) 所认为的, “隐私权包括保护私生活不受干扰及信息自主二个生活领域”、“信息自主, 即得自主决定是否及如何公开关于其个人的数据(信息隐私)”^③, 也有学者(彭礼堂、饶传平, 2006) 指出, 隐私权的内涵正从消极被动的“私生活不受干扰”发展为积极能动的“自己的信息自己控制”, 即资讯自决权的概念。^④

关于网络隐私权保护模式, 美国的迈克尔菲尔德(D. P. Michelfelder) 教授指出, 保护网络信息隐私的方式有三种: 一是靠技术保护; 二是靠自律保护; 三是靠法律保护。^⑤ 国内比较认可的张秀兰教授的观点, 即国际上存在两种对公民网络隐私权的保护模式, 一是以美国为代表的行业自律模式, 二是以欧盟为代表的法律规制模式。^⑥ 行业自律模式主要通过建立行业协会, 并由该协会出台行业自律的相关政策来保护互联网隐私。参与协会的成员必须自觉遵守行业自律政策, 有的行业协会还会向成员颁发认证组织的网络标志, 如美国加利福尼亚公司 TRUSTe 的在线隐私封条, 以告知网民该企业是遵守行业自律公约的。法律规制模式的基本做法是通过制定法律的方式, 从法律上确立网络隐私权保护的各项基本原则与各项具体的法律规定和制度, 并以此为基础, 采取相应的司法或者行政救济措施。^⑦ 如欧盟发布的《关于在信息高速公路上收集和传递个人数据的保护指令》(1999)、《关于电子通信领域个人数据处理和隐私保护的指令》(2002) 和《关于个人数据处理和自由流动的保护规则》(2012) 等。与美国专门的隐私验证机构不同, 中国没有第三方隐私验证机构。为了消除公众对隐私可能泄露的担心, 网络企业往往会制定隐私权保护政策(或者隐私条款、隐私保护协议、隐私声明), 以证明登陆与使用该网站是安全的, 用户的个人信息隐私不会被泄

① Savage, Scott J., and Donald M. Waldman, “Privacy Tradeoffs in Smartphone Applications”, *Economics Letters*, Vol. 137, 2015, pp. 171 – 175.

② Samuel D. Warren, Louis D. Brandeis, “The Right to Privacy”, *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193 – 220.

③ 王泽鉴《人格权的具体化及其保护范围·隐私权篇(中)》, 《比较法研究》2009 年第 1 期。

④ 彭礼堂、饶传平《网络隐私权的属性: 从传统人格权到资讯自决权》, 《法学评论》2006 年第 1 期。

⑤ D. P. Michelfelder, “The Moral Value of Informational Privacy in Cyberspace”, *Ethics & Information Technology*, Vol. 3, No. 2, 2001, pp. 129 – 135.

⑥ 张秀兰《网络隐私权保护研究》。北京: 北京图书馆出版社 2006 年版。

⑦ 徐敬宏《欧盟网络隐私权的法律法规保护及其启示》, 《情报理论与实践》2009 年第 5 期。

露。^① 互联网隐私保护政策成为隐私保护安全链中重要的一环。

当前有关网络环境下隐私政策的研究主要集中在隐私政策的原则与内容表述,以及隐私政策实践应用两大方面。在隐私政策的原则和内容方面,美国联邦委员会提出的网络业界保护个人隐私的四项原则(告知、许可、安全与完整、通道)^②,经济合作与发展组织(OECD)从公平信息实现的角度也给出了八项原则(搜集限制原则、数据质量原则、目的规范原则、使用限制原则、安全维护原则、公开原则、个体参与原则、责任原则)^③;Kwon将网络隐私政策内容分为类别(Categories)、目的(Purposes)、设置(Options)、保留(Retentions)的四个部分^④,Wang等则将隐私保护政策的访问控制策略的内容定义为一个六元组:主体(Subjects)、行为(Action)、资源(Resources)、目的(Purpose)、条件(Condition)、义务(Obligation)。^⑤

对隐私政策实践应用的相关研究则集中在对传统网站进行的分析,国内代表性研究主要有:谈咏梅、钱小平(2006)针对门户网站、BBS论坛、商务网站、游戏网站等四类网站进行研究,发现网站隐私政策制定标准参差不齐,没有网站对自己违反隐私政策将要承担的法律后果作出约定;^⑥郑嘉楠(2007)研究了Flicker(图片类)、Youtube(视频类)、Myspace(社区类)、Windows Live(博客类)、Orkut(交友类)共五家网站的隐私保护条款,发现针对儿童、不同国家用户和对非会员的隐私保护严重不足,提出我国Web2.0网站隐私保护的对策;^⑦徐敬宏(2008)对五家中英文网站的隐私声明进行文本分析,着眼于隐私声明的措辞、句型、句法特点和文本结构,发现英文网站相比中文网站来说,隐私声明的内容更为全面,使用更为便捷,内容更易理解,有专门的未成年人隐私保护内容;^⑧申琦选取我国社交类网站、电子购物网站等6类49家网站,运用内容分析法,实证地分析我国各类网站网络隐私保护政策的实际情况,发现我国网站隐私保护存在命名混乱、网站对于用户信息收集说明不清、未告知退出机制、缺失对未成年人隐私保护等问题;^⑨对移动APP隐私保护政策的直接研究尚付阙如,这也增加了本论文研究的理论和应用价值。

三、研究方法

(一) 研究对象

本文根据《互联网周刊》发布的《2016中国APP分类排行榜》^⑩、艾媒咨询发布的《中国APP活跃用户排行榜TOP400》^⑪以及猎豹全球智库2017年1月17日发布的《2016中国APP排行榜》,于2017年3月到4月期间考察了手机浏览器(5个)、新闻资讯类(7个)、影音播放类(8个)、社交应用类(10个)、移动电商类(13个)、金融理财类(10个)、旅行导航类(8个)、拍摄美化类(8个)、健康医疗类(8个)、办公存储类(9个)、生活服务类(10个)等11类96个我国境内能够下载和使用的

① 申琦《我国网站隐私保护政策研究:基于49家网站的内容分析》,《新闻大学》2015年第4期。

② 张秀兰《网络隐私权保护研究》,北京:北京图书馆出版社2006年版,第200页。

③ D. S. Allison, H. F. E. Yamany, M. Capretz "Metamodel for Privacy Policies within SOA", in *ICSE Workshop on Software Engineering for Secure Systems*, Vancouver, Canada, 19 May, 2009, pp. 40 - 46.

④ O. Kwon "A Pervasive P3P-Based Negotiation Mechanism for Privacy-Aware Pervasive E-Commerce", *Decision Support Systems*, Vol. 50, No. 1, 2011, pp. 213 - 221.

⑤ 刘百灵、万璐璐、李延晖《网络环境下基于隐私政策的隐私保护研究综述》,《情报理论与实践》2016年第9期。

⑥ 谈咏梅、钱小平《我国网站隐私保护政策完善之建议》,《现代情报》2006年第1期。

⑦ 郑嘉楠《Web2.0网站隐私权保护条款研究》,《图书馆学研究》2007年第11期。

⑧ 徐敬宏《网站隐私声明的真实功能考察:对五家网站隐私声明的文本分析》,《当代传播》2008年第6期。

⑨ 申琦《我国网站隐私保护政策研究:基于49家网站的内容分析》,《新闻大学》2015年第4期。

⑩ 《2015中国APP分类排行出炉 哪些APP稳居第一》,互联网周刊, http://internet.chinaso.com/detail/20150723/1000200003267621437609590525505402_1.html, 2015-07-23。

⑪ 《中国APP活跃用户排行榜TOP400》,艾媒咨询, <http://www.iimedia.cn/40687.html>, 2016-02-02。

iOS 移动网络客户端 APP 的隐私保护政策。

其中,将音频播放类和视频播放类归为“影音播放类”,将一般社交类和婚恋交友类归为“社交应用类”,将母婴电商类、外卖类、团购类、综合电商类和生鲜电商类归为“移动电商类”,将银行类和理财类归为“金融理财类”,将地图类和旅游出行类归为“旅行导航类”,将短视频拍摄类和图像美化类归为“拍摄美化类”,将运动、育儿、医疗、保健等归为“健康医疗类”,将办公软件、云盘存储、读书类归为“办公存储类”,将生活信息查找、装修、买车、求职、物流、交通等服务归为“生活服务类”。具体见表 1。

表 1 APP 移动应用分类

分类	应用
手机浏览器(5 个)	手机百度、UC 浏览器、QQ 浏览器、360 浏览器、Chrome
新闻资讯类(7 个)	腾讯新闻、搜狐新闻、今日头条、一点资讯、凤凰新闻、新浪新闻、人民日报
影音播放类(8 个)	酷狗音乐、酷我音乐、蜻蜓 FM、喜马拉雅 FM、优酷视频、爱奇艺、暴风影音、斗鱼
社交应用类(10 个)	微信、手机 QQ、新浪微博、人人网、陌陌、YY、世纪佳缘、珍爱网、知乎、豆瓣
移动电商类(13 个)	淘宝、京东商城、1 号店、苏宁易购、当当、亚马逊、中粮我买网、美团外卖、饿了么、口碑外卖、大众点评、百度糯米、支付宝
金融理财类(10 个)	拉卡拉、同花顺、挖财理财、东方财富网、新浪财经、工行手机银行、中国建设银行、农行掌上银行、招商银行、中国银行手机银行
旅行导航类(8 个)	百度地图、高德地图、谷歌地图、携程旅行、去哪儿旅行、同程旅游、途牛旅游、驴妈妈旅游
拍摄美化类(8 个)	美拍、微视、快手、秒拍、美图秀秀、in、天天 P 图、美人相机
健康医疗类(8 个)	小米运动、keep、乐动力、好大夫在线、微医、丁香医生、宝宝树孕育、妈妈网
办公存储类(9 个)	WPS Office、QQ 邮箱、网易邮箱大师、印象笔记、微办公、百度云、微云、掌阅 iReader、起点读书
生活服务类(10 个)	58 到家、赶集网、土巴兔装修、房天下、智联招聘、菜鸟物流网、汽车之家、全国违章查询、滴滴出行、摩拜单车

研究者将 96 个 APP 的隐私保护政策保存为文本文件或图片文件,同时记录从 APP 首页到隐私保护政策的点击数,将所得数据生成到 Excel 表格以进行内容分析。

(二) 研究内容

参照前文中所述关于隐私保护政策原则和内容的相关研究,再结合申琦(2015)和易斌(2011)^①的研究成果,本文将我国移动 APP 隐私保护政策研究分为隐私保护政策的一般情况和具体内容两部分。

隐私保护政策的一般情况涉及六个方面的问题:(1)是否有专门的隐私保护政策?(2)隐私保护政策名称的规范性;(3)获取隐私保护政策的便捷程度;(4)用户接受该政策的自主性;(5)更新时间的标注;(6)企业联系方式的提供。

隐私保护政策的具体内容涉及九个方面的问题:(1)收集数据内容;(2)收集数据目的;(3)收集数据方法;(4)数据披露条件;(5)数据保存期限;(6)数据安全保证;(7)用户权利;(8)未成年人隐私保护;(9)免责条款。

四、研究发现

(一) 我国移动 APP 隐私保护政策的一般情况(见表 2)

(1) 在 96 个移动 APP 中仅有 56 个(占比 58.3%)关于隐私保护政策的文本供用户查看,仍有

^① 易斌《读者隐私保护政策研究》,《情报理论与实践》2011 年第 8 期。

较多移动 APP 未发布隐私保护文本。

其中,所有收集浏览器的 APP 都有关于隐私保护的文本;排在第二位的是社交应用类 APP,占比达 80%;接下来是移动电商类、办公存储类、影音播放类、旅行导航类和金融理财类 APP,有隐私保护文本率占比在 60% 至 70% 之间;健康医疗类有隐私保护文本率为 50%;新闻资讯类、生活服务类和拍摄美化类隐私保护文本拥有率未能过半,其中拍摄美化类是隐私保护政策发布的重灾区,拥有隐私保护文本的占比仅有 12.5%。(见图 1)

表 2 各类 APP 隐私保护政策一般条款的制定情况 (n=56)

文件名称 (占比)	找到隐私保护政策的 点击次数(占比)	保护政策更新时间 (占比)	联系信息 (占比)
隐私声明 19.6%	1 次 7.1%	有 25.0%	客服电话 10.7%
隐私政策 39.3%	2 次 16.1%	无 75.0%	电子邮箱 28.6%
隐私协议 1.8%	3 次 35.7%		网址 26.8%
隐私保护声明 10.7%	4 次 33.9%		其他联系方式 16.1%
其他 28.6%	5 次 7.2%		两种以上联系方式 21.4%
			无联系方式 51.8%

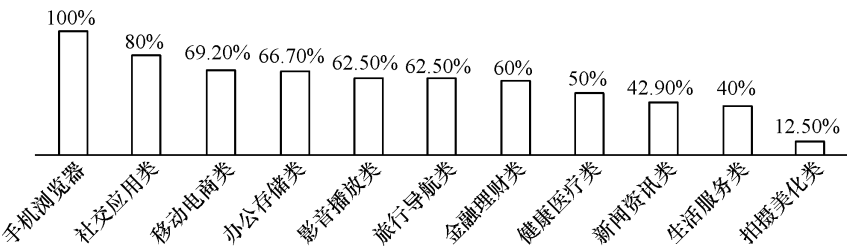


图 1 有隐私保护文本的 APP 分类占比

(2) 我国联网 APP 隐私保护采用的名称不够规范,28.6% 的 APP 隐私保护采用的是“其他”类名称,包括“法律声明”、“服务协议”、“用户许可协议”、“关于”、“服务条款”、“用户需知”等。它们没有单独列出用户隐私保护政策或者隐私保护声明,隐私保护政策的文本依附在其他相关管理条例和说明的条款中。

(3) 用户在查找 APP 隐私保护政策时非常不便利。从用户找到 APP 网络隐私保护政策的次数来看,用户平均要点击 3 次才能找到相关的隐私保护政策。超过三分之一的 APP 需要点击 3 次或 4 次才能到达隐私保护政策的文本(占比分别为 35.7% 和 33.9%),3.6% 的 APP 需要点击 5 次。甚至有些 APP 必须在用户注册成为会员后,才可以查看隐私政策,意味着用户在不知该 APP 会对个人隐私数据做出何种处理的情况下就要提交信息,这是非常不合理的。

(4) 仅 25.0% 的 APP 指出了隐私保护政策的更新时间,大多数的 APP(占比 75.0%) 在其隐私保护政策的文本中没有对更新时间和有效时间做出相关说明。这说明我国移动互联网隐私保护还处于不成熟阶段。

(5) 过半数的 APP(占比 51.8%) 未在隐私保护政策中注明相关的联系信息,没有考虑到用户遇到隐私侵害或是对隐私保护政策产生疑惑的情况。这表明此类 APP 的开发者没有将隐私保护政策当作对用户的承诺和保护,而仅流于形式,没有起到真正的保护作用。有 21.4% 的 APP 留下了

两种以上的联系方式,说明这些 APP 开发者已经深刻意识到为用户提供服务,对用户负责的重要性。

(二) 我国移动 APP 隐私保护政策的基本内容

(1) 收集数据内容。通常来说,移动 APP 需要收集的数据内容,包括个人基本信息(姓名、生日、性别、住址、电话号码、电子邮箱),身份信息(身份证、军官证、护照、驾驶证等),面部特征,网络身份标识信息(系统账号、IP 地址、密码、口令、口令保护答案),个人财产信息(交易和消费记录、虚拟财产信息),通讯录,个人上网记录(包括网站浏览记录、软件使用记录、点击记录),个人常用设备信息(包括硬件型号、设备 MAC 地址、操作系统类型等),个人位置信息(包括行程信息、精准定位信息、住宿信息、经纬度等)等。在这些信息中,有一部分属于个人敏感信息,比如财产信息、身份信息、面部识别特征、个人联系方式等,一旦泄露、非法提供或者滥用可能危害人身和财产安全,需要得到保护。调查结果显示,在有隐私保护政策的 56 个 APP 中,只有 5 个移动 APP 没有收集数据的内容,占比 8.9%。

(2) 收集数据目的。网络服务商在收集数据的同时,一般都要交代收集数据的目的,包括实现部分网络功能、满足用户个性化需求、用于产品和服务调查、为用户提供安全保障等。绝大部分移动 APP 交代了收集数据的目的,仅有 1 家没有。

(3) 收集数据方法。通常来说,移动 APP 收集数据的基础方法有两大类:用户主动提供个人化数据;移动 APP 通过 Cookie、Beacon、Proxy 等方式获取用户的数据。调查对象中有 14 家移动 APP(占比 25%)没有交代收集数据的方法,可能也是鉴于技术性强而回避这一部分。与此相对应的,也有 11 个移动 APP(占比 19.6%)为了让用户理解,特别对相关技术词汇进行了详细解释,如腾讯网、高德地图等,充分体现了对用户知情权的尊重。

(4) 数据披露条件。网络运营商负有保护用户个人数据安全的义务,不能随意向第三方提供用户的个人数据。一般来说,网络运营商进行披露用户数据的前提有两个:第一是经过用户许可,第二是某些特殊情况,如涉及国家安全、违法犯罪、权利滥用等。在 56 个 APP 中,仅有 2 个(占比 3.6%)未交代数据披露条件,可见大部分移动 APP 在制定隐私政策时都考虑到了这些因素。

(5) 数据保存期限。移动 APP 一方面要注重用户数据的保存,方便用户和自身调取,另一方面也要注意数据保存期限,在完成了特定的任务之后,有些数据是要予以删除和销毁的。对此,英国 1984 年实施的《数据保护法》规定“依任何目的处理个人数据者,其数据保留期限不得超过其取得目的的必要期限。”由于网络存储数据的大容量和便捷性,数据保存期限这一项经常为不少网络运营商所忽视。调查对象中,有 36 家移动 APP(占比 64.3%)没有设定数据保存期限。

(6) 数据安全保证。互联网上存在着黑客、病毒等不安全因素,容易发生用户隐私被窃取的情况,这几年用户信息和银行账号集体泄露事件,也让网民对网络数据安全缺乏信心。网络运营商负有保护用户个人数据安全的义务,一方面要运用各种技术、自律和法律手段保护用户数据安全,另一方面也要提醒用户网络存在的风险。总体而言,各大网络运营商都非常重视数据安全问题,调查对象中仅有 8 个移动 APP(占比 14.3%)没有将数据安全保证写入隐私保护政策中。

(7) 用户权利。用户对自己的个人信息,有随时查询、补充、更正和删除的权利,是否详细规定了用户权利是检验隐私政策内容是否完备的重要标准之一。在 56 个有效对象中,39 个移动 APP(占比 69.6%)将用户权利写入了隐私保护政策中,表明大部分网络运营商对用户权利的重视。

(8) 未成年人隐私保护。保护未成年人隐私已经成为国际社会共识,各国都有相关法案予以规定。《中华人民共和国未成年人保护法》第三十九条规定,任何组织或者个人不得披露未成年人的个人隐私。因此,我国的移动 APP 隐私政策中也应单独设计未成年人隐私保护问题。这个部分也是比较容易被网络运营商们忽视的,22 家移动 APP(占比 39.3%)没有关于未成年人隐私保护内容,在社交应用、金融理财、健康医疗和生活服务四个领域较为突出。

(9) 免责条款。在一些特殊情况下,网络运营商无法保障用户的个人数据安全,如用户自身原因导致的个人数据泄露,或者遇到政府管制、黑客攻击等不可抗力,由于运营商本身没有过错,因此也不需要承担责任。为了避免事后出现纠纷,网络运营商通常也会将这类免责条款写入隐私保护政策中,用以保护自身权益。在有效对象中,24个移动APP(占比42.9%)没有免责条款,自我保护意识不够强。

五、主要结论和建议

(一) 隐私政策水平参差不齐

在调查对象中,有的移动APP隐私政策醒目、清晰、详细而且专业,部分移动APP还提供了更便利的在线“一站式”撤回和关闭授权,在线访问、更正、删除其个人信息,在线注销账户等功能,如京东商城、滴滴出行、淘宝网、腾讯微信等;有的移动APP隐私政策内容非常简单、隐蔽、模糊和随意,如同花顺、当当网等。通常来说,大企业开发的APP隐私保护水平高于小企业,如淘宝APP还使用了双语告知隐私政策;国际企业APP的隐私保护政策比大部分国内企业APP更为专业和详细,如来自Google的APP产品Chrome和谷歌地图等;运营时间较长的APP隐私保护政策比创立不久的APP要完善,如口碑外卖(2013年创立)和饿了么(2009年创立)同属外卖类电商,但口碑外卖的隐私保护政策十分简单,饿了么对隐私保护的规定相对全面。

数据安全和用户信息保护是对互联网企业的核心基本要求,隐私权政策的完善和提升不仅要符合法律法规和监管规定,更是维护市场信心和用户信任的基石,也是企业行稳致远的核心竞争力,最终受益最大的还是企业。^①各大企业APP应该加强对隐私保护政策的制定与完善,具体而言,可以参照国际著名企业的做法,制定规范、完整、专业、清晰的隐私保护政策,让用户能够准确清楚地了解个人信息收集、使用、分享和保护的流程,减少用户的隐私顾虑,增加用户对企业和产品的信心。

(二) 霸王条款现象仍然存在

不少APP推行霸王条款,强行要求用户接受相关隐私政策,如果用户不接受会强制退出APP,或者被取消相关服务;有些APP隐私政策内容也极为霸道,较少考虑用户的需求,强行规定用户的个人信息可用于不合理的商业用途,并拒绝承担任何用户隐私泄露的责任。如珍爱网规定“您在缔结本协议时已理解并同意,您在本网站上公开发布的个人信息,任何登陆到本网站的第三人均可查看”、“一旦您使用珍爱网或成为会员(无论是付费还是免费),则表示您已许可我们将这些信息披露给我们的附属公司、母公司和相关联的第三方商业机构,以及其他和我们处于共同公司控制权的有关联的法律实体和商业机构。”又如快手APP规定“如果您不同意本隐私权政策任何内容,您应立即停止使用快手平台服务……快手可能随时修改本隐私政策的条款,该等修改构成本隐私政策的一部分……快手可随时根据实际情况有权自行决定以任何理由不经事先通知的中止、终止向用户提供部分或全部快手服务,暂时冻结或永久冻结(注销)用户的账户在快手的权限,且无须为此向用户或任何第三方承担任何责任。”

对于这种情况,一方面,企业应该本着“用户中心”、“服务至上”的原则,始终将用户的个人权益放在首位,尊重用户才能获得用户的支持,也能够尽可能避免法律纠纷;另一方面,网民也要增强自己的隐私保护意识,敢于主张自己的合法权益,明确自己对隐私权的合理期待,提升自己的议价能力,获取更为安全的网络服务。^②

① 余瀛波《10款常用APP集中更新隐私条款》,《法制日报》2017年9月25日,第6版。

② 申琦《我国网站隐私保护政策研究:基于49家网站的内容分析》,《新闻大学》2015年第4期。

(三) 缺乏隐私政策协商机制

当前,面对网站单方面给出的隐私政策,用户只能选择 YES/NO,而不能对披露信息的种类与使用方式进行选择,这种方法已出现严重弊端。^① 用户只能全盘接受该政策,或者全盘否定该政策,而且大部分用户在否定即可能无法获得服务的威胁下会选择全盘接受,无法顾及不同的人对信息披露接受的程度要求,一定程度上影响到用户对 APP 的使用体验。

加强用户与网络运营商的沟通,建立隐私政策协商机制是解决该问题的一种有效方式。所谓隐私政策协商,就是将网络运营商请求获取的用户信息与用户的隐私偏好进行比较与商讨,最终双方达成一致的一系列活动。^② 个性化的隐私协商可以为用户提供个性化的服务,这种协商可以通过技术平台来实现。W3C 组织提出了 P3P(Platform for Privacy Preferences)个人隐私偏好平台,P3P 通过匹配 Web 站点的隐私策略(Privacy Policy)和用户的隐私偏好(Privacy Preference)来决定是否允许将用户的隐私数据提供给 Web 站点使用,向用户提供个人隐私信息在保护性上的可操作性。^③ 尽管这种技术早已有之,但是由于需要手动设置、工作量大,未能被大部分移动 APP 运用。网络运营商们在建立“用户中心”发展策略之后,不可忽视这些细节的处理。

(四) 隐私保护效果不够理想

尽管有不少移动 APP 制定了隐私政策,但是,由于缺乏专门监督机构和完善监督机制,在现实中并没有按照规定严格执行隐私政策。有的 APP 运营商会将隐私政策隐蔽化处理或将隐私政策制定得冗长深奥,增加用户阅读难度;有的会擅自修改隐私政策而不告知用户;有的会不当使用用户隐私数据;有的则没有积极采取实际技术手段进行隐私保护……隐私保护未达到理想效果。

建立隐私保护政策只是移动互联网时代个人信息保护的其中一步,要实现隐私保护效果,需要多个主体努力。首先政府需要进行监督和管理,包括引导网络企业自律、依法对侵权行为进行惩戒、赋予应用平台审核责任、推进和鼓励保护网络隐私权的新技术开发和利用等;其次是需要加强第三方隐私保护机构的监督,设立类似于美国 TRUSTe 和 BBBOnline 这样的行业自律组织,认证并监督网络机构的隐私政策,完成隐私执行和效果评估,参与解决消费者争端和用户隐私问题;最后企业要加强自律,可以学习美国等发达国家的做法,在企业内部设立专门负责处理用户隐私权相关事宜,并直接对企业最高领导人负责的首席隐私官(Chief Privacy Officer, CPO)^④,实现将用户数据尽可能转化为公司财产,又不侵犯用户隐私权的理想效果。

(广东外语外贸大学新闻学院李蓉协助本文的资料整理及写作,特此致谢)

[责任编辑 王 桃 责任校对 李晶晶]

① Liu Y., “User Control of Personal Information Concerning Mobile-App: Notice and Consent?”, *Computer Law & Security Review*, Vol. 30, No. 5, 2014, pp. 521 – 529.

② M. Johnson, J. Karat, CM. Karat, K. Grueneberg “Optimizing a Policy Authoring Framework for Security and Privacy Policies”, *Proceedings of the Sixth Symposium on Usable Privacy and Security*, Redmond, USA, July 14 – 16, 2010, PP. 1 – 9.

③ 战照鹏、付长龙、姚全珠《基于 Pareto 最佳解的 P3P 隐私协商机制研究》,《计算机应用研究》2006 年第 2 期。

④ 徐敬宏《美国网络隐私权的行业自律保护及其对我国的启示》,《情报理论与实践》2008 年第 6 期。