我国移动应用软件隐私政策的合规审查及完善

——基于49例隐私政策的文本考察

李　延　舜*

摘要：应用软件隐私政策不仅是应用软件服务协议的一部分，还是应用软件企业承担数据保护责任的体现。应用软件的隐私政策除具有合同属性、社会承诺属性外，还应是“公司治理”与“行业自律”的一种体现。我国应用软件隐私政策虽然受法律的影响在文本上进行了调整，但是仍广泛存在隐私政策出场、数据收集、数据留存期限、数字广告推送、数据安全保护以及数据的共享、披露和转移等方面的合规问题，应从“克服集体行动难题”“问责”以及“行政监管与公司治理、行业自治相结合”3个方面来实现应用软件隐私政策从文本走向实践的合规审查。

关键词：应用软件　　隐私政策　　合规审查　　公司治理　　社会责任

近年来，伴随智能手机的普及，各种各样的应用软件（App）应运而生，无论是购物、社交、金融、游戏还是旅游，都有种类繁多的应用软件等待消费者选择、安装、使用。在应用软件安装使用的过程中，有个“隐私政策”的链接，而此类隐私政策往往涉及个人信息的收集、存储和使用。那么隐私政策中的消费者个人信息收集、存储和使用的合规性如何呢？本文选择并搜集、整理了49例国内常用应用软件隐私政策，拟从9项核心指标和6项一般指标入手，对这些应用软件隐私政策的合规性进行考察，以期揭示相关的合规性问题，并就隐私政策的合规性贯彻落实提供若干建议。

一、问题的提出

2018年5月25日生效的欧盟《一般数据保护条例》（以下简称《欧盟条例》）第47条规定了“有约束力的公司规则”，也称“隐私政策”，[①]该条赋予监管机关对符合条件的公司规则予以批准的义务。换句话讲，大数据依托企业制定的隐私政策必须符合法律法规的规定，集中体现在《欧盟条例》第47条第2款详细阐述的14项内容上。[②] 那么，隐私政策在应用软件及其背后的互联网企业经营中到底扮演什么角色呢？或者说，隐私政策的属性为何？已有的研究成果将其视为用户协议的一部分，如有学者在对现有隐私政策进行两分的基础上，认为隐私政策属于“网站与网络用户双方之间的协议，……用户有提交个人资料的义务，同时也有要求条款提供者提供网络服务的权利；而条款提供者有按照条款规定保护用户隐私、提供服务的

*　河南大学法学院副教授

基金项目：司法部国家法治与法学理论研究项目（17SFB2005）、河南省哲学社会科学规划项目（2017BFX014）

①　“隐私政策”是大多数应用软件或网站所采用的称呼，除“隐私政策”外，“隐私保护指引”“服务协议及隐私条款”“隐私权政策”“个人信息保护政策”等皆表达相同的含义。

②　《欧盟一般数据保护条例》第47条第2款规定，有约束力的规则至少应当明确：（1）企业集团或其他经济主体及其联系方式，（2）有关数据转移的规定，（3）规则的法律约束效力，（4）对一般数据保护原则的适用，（5）数据主体的权利以及行使这些权利的方式，（6）责任的承担及免除情形，（7）如何将公司规则提供给数据主体，（8）数据保护官的任务，（9）申诉程序，（10）公司内部如何实现对规则的遵守，（11）数据报告和记录规则变化的机制，（12）如何与监管机构合作的机制，（13）向监管机构报告第三国主体可能引起负面影响的机制，（14）对员工进行适当数据保护培训的机制。

义务，同时也享有合理使用个人隐私资料的权利”。[①] 有些应用软件的隐私政策文本更是旗帜鲜明地点明了这一点，如《拼多多隐私权政策》第1条指出，“本《拼多多隐私权政策》是《拼多多服务协议》组成部分”。那么将隐私政策视为用户协议一部分的观点有无问题呢？答案是肯定的。因为如此一来，该政策就属于“格式条款”的内容，消费者要么同意，要么离开，协议所应有的“协商”“合意”在应用软件安装使用过程中荡然无存。

要想消除经营者和使用者在地位上的不平等，必须赋予隐私条款社会属性。从本质上讲，由于隐私政策是应用软件经营者对消费者个人数据收集、存储、使用、转让的说明及承诺，因此隐私政策的合同属性应让位于社会承诺属性。一方面，消费者个人信息蕴含着社会价值，如购买记录和信用记录，因而名义上属于企业权利“分内之事”的隐私决策行为也必须符合公共利益。因为决策虽是私人的，但却具有公共效果。[②] 另一方面，隐私政策的社会承诺属性意味着深刻的个人信息保护理念的转变，数据保护规则“不是由个体决定的，而应当是由社会共同决定的，……个人信息的社会控制意味着个人信息的使用由社会习惯或法律决定，而不是由个人意志决定”。[③]当越来越多的人对应用软件收集和使用个人信息产生“知情”的意识以及问责的态度时，应用软件隐私政策就呈现出从纯粹的阅读文本向功能文本转变的趋势。换言之，即便用户不怎么阅读隐私政策，但是上至监管机构，下至消费者，中至隐私权倡导者及媒体等，都可以将应用软件隐私政策放在聚光灯下反复打量、评价，并且这一评价成为企业社会形象的一部分。此外，隐私政策亦是问责和执法机制的依据。因为“除了法律可能具有的规定之外，它们还设定了商业使用数据的界限，根据消费者保护法规确定了可实施的法律责任。它们对信息披露的要求可以迫使公司对它们的隐私实践进行评估，并在其对消费者信息的处理中强调纪律”。[④]

除合同属性、社会承诺属性外，应用软件隐私政策还是一种“公司治理”与“行业自律”的体现。一方面，即使个人信息保护法制（或数据保护条例）再完美，其目的的实现也有赖与经营者（公司）内部治理的对接，法律对应用软件背后的经营者提出了约束，如前述“有约束力的公司规则”、数据保护官的设置等，公司需要以隐私政策的形式对公民数据隐私作出肯定性的回应；另一方面，个人数据收集和利用的组织需要对行业行为予以规范，不管经营者是出于行业健康发展的动机，还是担心政府的规制可能比自我约束更严苛，抑或源于更纯洁的理由（如他们坚信必须依照道德标准经营），经营者都力图在政府规制之前“先发制人”，通过制定或修改隐私政策，向政府和社会传达他们尊重并保护公民隐私的态度。在本文搜集的49例隐私政策文本中，除5例隐私政策文本没有注明制定（修改）时间外，其他44例皆在《中华人民共和国网络安全法》（以下简称《网络安全法》）生效后制定或修改；而在这44例中，有39例在《欧盟条例》生效后进行了修订或更新，可见法律对大数据依托企业所设义务带来的重要影响。

大数据时代，每个人的个人数据都已不再属于自己，而是商业链条上不可或缺的一环。移动应用软件的开发、应用使得在线活动（如社交、购物、订票、游戏、娱乐等）更便捷（它摆脱了网线的束缚），也变得更智能，但也由此，经营者于悄无声息间完成了对消费者的数字监控。以在线购物为例，消费者“对商品的每一次点击、浏览都会留下足迹，甚至浏览某一商品的时间长短，都会被记录在案。如此，在线销售者根本就不需要认识消费者本人，只需要通过其‘足迹’就可判断其消费层次及消费偏好”。[⑤] 即使那些不需要注册、提交个人信息就能安装使用的应用软件（如高德地图、百度地图等），也不过是一笔“浮士德式”交易，[⑥]所谓的“免费”并不是真的免费。在这样的交易中，应用软件提供的服务或内容实际上是引诱用户允许其监

① 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。

② 参见[美]弗兰克·H.伊斯特布鲁克等：《公司法的逻辑》，黄辉编译，法律出版社2016年版，第252页。

③ 高富平：《个人信息保护：从个人控制到社会控制》，《法学研究》2018年第3期。

④ [美]马克·罗滕伯格等主编：《无处安放的互联网隐私》，苗森译，中国人民大学出版社2017年版，第170～171页。

⑤ 李延舜：《个人信息财产权理论及其检讨》，《学习与探索》2017年第10期。

⑥ 浮士德与魔鬼交易的故事可以追溯到中世纪，在很多不同的文学作品中都有所体现，如克里斯托弗·马洛和约翰·歌德的作品。在这些神话中，浮士德与魔鬼达成了一份协议，他愿意将灵魂割舍给魔鬼墨菲斯特以换取财富、权力或者其他形式的恶魔的支持。现在，“浮士德式”交易意味着一份你所同意的交易，为了获取眼前利益而不顾潜在损失或者长期后果。

控在线活动、了解其偏好、获取其观点并向其发送定向广告的诱饵。如此,“通过为其他人提供单方面的利益,一个人就积累了他能够利用的自愿服从的资本。在他持续地为他们提供利益的意义限度内,不管在什么时候,只要他愿意,他都可以将他的意志强加在他人身上”。[①]这种交易构成应用软件商业模式的基础。

应用软件背后的经营者并不会因为隐私政策的出台就自动获得个人数据收集与利用的正当性,更不会依据隐私政策文本就免于承担侵权责任。应用软件隐私政策是否符合法律的规定并与之对接?是否担负起了其应有的功能?是否在保护个人数据方面取得预期的成效?这既需要法理的审视,又需要实践的检验。《网络安全法》第 41 条第 1 款规定了隐私政策的基本要求——公开、明示、同意,但截至目前,并无任何监管部门对这些隐私政策进行起码的合规性审查。中国消费者协会曾于 2018 年 7 月 17 日至 8 月 13 日组织开展“应用软件个人信息泄露情况”问卷调查,调查结果显示手机应用软件存在过度采集个人信息的趋势,且应用软件隐私政策的“合规性”及“标准化程度”有待提高。[②] 2018 年 11 月 28 日,中国消费者协会再次在北京召开新闻发布会,通报 100 款应用软件的个人信息收集与隐私政策测评情况,而测评结果极不乐观。[③] 在隐私裸奔的大数据时代,作为现代公司治理体系中的重要一环,隐私政策的合规必然成为数字经济发展的重要内容。消费者日益重视数据隐私保护的需求,将会在市场竞争中自动为那些拥有完善隐私政策的经营者加码。因为“如果每一个公司都真心实意地遵守这些政策条款,那么可以下结论:他们表现出了对隐私权的尊重”。[④]

当然,对隐私政策的重视并不仅仅出于对经营者的不信任,还有更深层次的考量。早在 1997 年互联网发展初期,时任美国总统的克林顿就批准并公布了《全球电子商务框架报告》。该报告强调,在保护互联网隐私权方面私营企业应当起到主导作用,政府支持私营部门为此而进行自我规范的努力,这种努力体现在建设有意义的、对消费者友善的隐私保护环境中。[⑤] 隐私政策正是这样一种规范,它绝不仅是一种束之高阁的宣示性文件,即使应用软件用户阅读它的比例很少,它也是平衡消费者与经营者势力比、避免商业上的数据监控形成的重要内容。因为隐私政策中经营者的义务清单和用户的权利条款是明白、清晰且有效的。过于重视个人数据收集和利用带来的红利,而忽视应用软件背后因技术、资本、地位而形成的权力鸿沟,那对于数字经济发展来说,“反而可能像是要倒掉婴儿澡盆里的水,却把小婴儿倒掉一般。这是以一种虽然可以理解、但并不健康的反应,走向了另一个极端——从无所不在的过去,走向了完全不顾其他的现在”。[⑥]

二、应用软件隐私政策的文本合规考核

(一)合规考核文本的选择

2018 年 7 月 12 日,全球领先的新经济行业数据挖掘和分析机构艾媒咨询发布了《2018 上半年中国 APP 排行榜》,因为应用软件种类繁多,笔者选取应用软件遵循两个前提,一是所选应用软件位列各自所属类别榜单的前 10 名,二是所选应用软件大多为普通民众所知悉。因此,共在 8 个类别中选取 49 款应用软件,并对其隐私政策进行分析(隐私政策文本获取时间截至 2019 年 7 月 25 日)。

---

① [美]彼得·M.布劳:《社会生活中的交换与权力》,李国武译,商务印书馆 2012 年版,第 71 页。

② 此次调查共计回收有效问卷 5 458 份,其中,26.2%的受访者表示从未阅读过应用软件隐私政策,“不授权就没法用”是受访者“从不阅读”的最主要原因,占 61.2%。另外,近 7 成受访者认为手机应用软件在自身功能不必要的情况下获取用户隐私权限,而消费者个人信息安全意识虽然较强但是缺乏有效的保护手段。参见中国消费者协会:《APP 个人信息泄漏情况调查报告》,http://www.cca.org.cn/jmxf/detail/28180.html,2018-08-29。

③ 报告显示,在收集个人信息方面,10 类应用软件普遍存在涉嫌过度收集个人信息的情况,59 款涉嫌过度收集“位置信息”,28 款涉嫌过度收集“通信录信息”,23 款涉嫌过度收集“身份信息”,22 款涉嫌过度收集“手机号码”。而在隐私政策方面,34 款应用软件没有隐私条款,47 款应用软件隐私条款内容不达标。参见中国消费者协会:《中消协在京发布〈100 款 APP 个人信息收集与隐私政策测评报告〉》,http://www.cca.org.cn/zxsd/detail/28309.html,2018-11-28。

④ [美]理查德·斯皮内洛:《铁笼,还是乌托邦——网络空间的道德与法律》,李伦等译,北京大学出版社 2007 年第 2 版,第 148 页。

⑤ 转引自汪靖:《不被洞察的权利——互联网精准广告与消费者隐私保护研究》,复旦大学出版社 2016 年版,第 143 页。

⑥ [英]麦尔荀伯格:《大数据·隐私篇:数位时代,「删去」是必要的美德》,林俊宏译,台湾远见天下文化出版股份有限公司 2015 年版,第 166 页。

表1.应用软件隐私政策文本的选取

购物类	天猫、唯品会、苏宁易购、小米商城、蘑菇街、聚美优品、手机淘宝、美团、拼多多、京东商城
互联网金融类	支付宝、翼支付、中国工商银行、中国建设银行、农行掌上银行
新闻资讯类	今日头条、腾讯新闻、网易新闻、凤凰新闻、天天快报
旅游通讯类	百度地图、高德地图、滴滴出行、携程旅行、去哪儿旅行
搜索类	百度、搜狗、360搜索、必应
社交交友类	微信、百度贴吧、QQ、陌陌、(新浪)微博
生活服务类	墨迹天气、铁路12306、饿了么、QQ阅读、58同城
休闲娱乐类	爱奇艺、腾讯视频、QQ音乐、酷狗、抖音短视频、美图秀秀、西瓜视频、火山小视频、全民K歌、快手

(二)合规考核指标的分类与考察

应用软件隐私政策合规与否的判断需要一些指标,符合(满足)了这些指标,我们可以作出其合规的结论。这其中,又可分为核心指标与一般指标,而该分类的作出主要是基于是否关乎实体性权利义务关系。如下表:

表2.核心指标名称及属性

序号	核心指标名称	属性
1	敏感信息提示	用户知情权、经营者透明义务
2	未成年人信息处理	经营者义务
3	收集数据目录	用户知情权、经营者透明义务
4	设备权限调用	用户知情、同意权,经营者透明义务
5	用户权限	用户数据权利
6	经营者对用户数据共享、披露与转移的说明	用户知情权、同意权,经营者透明义务
7	数据存储	用户知情权、经营者安全义务
8	免责条款	经营者的单方免责声明
9	安全事件处理及应急预案	经营者义务、监管部门监管职责

表3.一般指标名称及属性

序号	一般指标名称	属性
1	是否有独立隐私政策	关涉重视程度及显著性
2	浏览器缓存或信标使用说明	经营者透明义务
3	广告推送及撤销的说明	用户选择接受还是不接受的方式
4	联系方式	用户交涉途径
5	纠纷处理	用户与经营者间的纠纷处理选择
6	是否经过权威认证	关涉“标准化”、行业认证标志

说明:核心指标的来源有三,即用户权利、应用软件经营者义务及监管部门职责,这是判断一项隐私政策是否合规的关键。一般指标的来源比较多元,并不直接指向隐私关系主体间的实体性权利义务关系,而是辅助并完善一项隐私政策,使之具备可操作性;或者说,让其真正成为有效力的、可诉而非束之高阁的规范性法律文件。总之,两者类似汽车的发动机与车轮等配件,重要性有所不同但又缺一不可。

(三)合规考核的结果与结论

1.核心指标方面

表 4.应用软件隐私政策中核心指标内容出现次数及占比

应用软件类型	敏感信息提示	未成年人信息处理	收集数据目录	设备权限调用说明	用户权限	经营者对用户数据共享、披露与转移的说明	数据存储	免责条款	安全事件处理及应急预案
购物类(10)	3	9	10	5	10	10	7	0	6
互联网金融类(5)	4	5	5	2	5	5	3	0	4
新闻资讯类(5)	4	5	4	1	5	5	4	0	4
旅游通讯类(5)	4	5	5	1	4	5	4	0	4
搜索类(4)	1	4	4	0	4	4	3	0	3
社交交友类(5)	4	5	5	0	5	5	4	0	3
生活服务类(5)	4	5	5	1	5	5	3	3	1
休闲娱乐类(10)	9	10	10	0	10	10	9	0	8
占比(49)	59.2%	98%	98%	22.4%	98%	100%	77.6%	6.1%	67.3%

2.一般指标方面

表 5.应用软件隐私政策中一般指标内容出现次数及占比

应用软件类型	是否有独立隐私政策	浏览器缓存或信标技术说明	广告推送及撤销的说明	联系方式	纠纷处理	是否经过权威认证
购物类(10)	10	10	6	6	6	5
互联网金融类(5)	4	4	3	5	1	1
新闻资讯类(5)	5	5	1	5	2	0
旅游通讯类(5)	5	5	0	4	1	2
搜索类(4)	4	4	1	3	0	0
社交交友类(5)	5	5	2	4	1	2
生活服务类(5)	5	5	1	4	0	0
休闲娱乐类(10)	10	9	5	10	2	3
占比(49)	98%	95.9%	38.8%	83.7%	26.5%	26.5%

说明:表 4 和表 5 的数字来源是在该类型应用软件隐私政策中出现该指标(条款)的次数。以核心指标中“敏感信息提示”为例,购物类中的“3”是指 10 例购物类应用软件隐私政策中仅有 3 例含有“敏感信息提示”指标。

3.合规考核的结论

虽然核心指标(条款)或一般指标(条款)的存在并不意味着该指标(条款)的内容合规,但是起码说明经营者已认识到该指标的重要性或不可或缺,也多少能反映出该款隐私政策的完善程度。上述数据告诉我们:(1)应用软件经营者越来越重视隐私政策。9 项核心指标+6 项一般指标的考察几乎覆盖了隐私政策的各个方面,甚至超出了前文所述《欧盟条例》第 47 条的内容。即便如此,所选取的应用软件隐私政策在各项指标上均有所体现,并且有些隐私政策已经相对比较完善,包含 15 项指标中的绝大多数。(2)通过对 49 例隐私政策文本的比较,笔者发现隐私政策与产品、场景的结合越来越紧密。例如,《京东隐私政策》与《天猫隐私政策》比较接近,《携程旅行隐私政策》与《去哪儿旅行隐私政策》比较类似,《爱奇艺隐私政策》与《酷狗隐私政策》趋同。这既意味着不同的应用软件收集和利用个人数据的范围、方式有所不同,隐私政策呈现出行业化、定制化和个性化的趋势,同时也意味着应用软件经营者不再全盘照搬行业标杆企业隐私政策,而是从自身提供的服务出发,因地制宜制定或修改隐私政策。这对消费者隐私权保护及数字经济发

展都是一个好的开端，它实现了由“自发”到“自觉”的转变。(3)虽然绝大多数应用软件(98%)都有相对独立的隐私政策，但是隐私政策的条款并不完备，尤其是9项核心条款，直接涉及经营者和消费者之间权利义务关系以及监管部门职责的内容。而6项一般条款的数据并不出色，这大大超出笔者在做文本实证研究之前的预期。如果说核心条款的拟定还需要些专业知识的话，那么一般条款的拟定几乎没有多少技术含量。(4)不同类型的应用软件隐私政策差异很大，市场化程度越高、竞争越激烈以及民众使用频次越多的应用软件，其隐私政策相对越完善，反之，其隐私政策表现越差。以购物类应用软件为例，口碑较好的天猫和京东两款应用软件的隐私政策在49例隐私政策中位居前列。(5)经营者与消费者权限、地位上的不对等在隐私政策中体现得较为明显。以核心指标(表4)为例：当前最为消费者关心的“设备权限调用说明”指标仅为22.4%；“收集数据目录”以及“经营者对用户数据共享、披露与转移的说明”两项指标虽然高达98%和100%，但是因其具有无法协商、无权修改、只能被动接受等特点而沦为经营者表面上公开、透明义务的展示；虽然“用户权限”指标已达到98%，但是数字的美好并不能掩盖消费者数据权利匮乏的现实。一方面，从名称上看，绝大多数隐私政策文本中用“您如何管理自己的信息”之类的名称代替“用户权限”，这说明经营者对用户的数据权利观念并不强烈；另一方面，即使如《抖音短视频隐私政策》《西瓜视频隐私政策》用“你的权利”来指称“用户权限”，但其真正的权利选项并不多。这说明，经营者制定隐私政策始终以经营者的利益为上。

三、应用软件隐私政策文本合规问题的实践解读

如果说上一部分的数据仅指向隐私政策中是否具备特定指标(条款)的“形式审查”的话，那么本部分将进行隐私政策具体条款的“实质审查”。以“核心指标+一般指标”为分析工具的量化研究表明隐私政策的完善之路还很遥远，但有些指标并不难完成，如核心指标中的“敏感信息提示”“未成年人信息处理”，一般指标中的“浏览器缓存或信标技术说明”等。事实上，在隐私政策文本中真正值得注意或者说亟须改进的问题主要集中在以下6个方面。

(一)隐私政策的出场问题：从“不知情、没得选”到“知情、同意”

如果说网站上的隐私政策通常能在网页上相对容易地找到，那么应用软件隐私政策则需要在手机上安装后(或安装过程中)才能找到。也就是说，要么在应用软件安装完成后，从注册或设置界面中通过链接寻找，要么在安装过程中遇到用户协议或隐私政策这个拦路虎，而用户需要勾选或默认同意该隐私政策才能进一步完成安装。无论哪一种，都是在事实上剥夺用户的事先知情权与选择权。因为尽管在隐私政策页面上有“同意”与“不同意”的选择项，但如果用户真的勾选“不同意”，那么下一步极有可能是“退出”或“重新选择”，从而不同意选项形同虚设。正如学者指出的那样：“就个人享受数据企业提供的数据产品和服务而言，虽然数据企业依法应取得被收集个人数据的自然人的同意，但作为消费者的自然人并没有协商的空间和议价的能力。绝大多数时候，数据企业给消费者的选择项只有两个：留下或离开。”[①]显然，这种隐私政策的出场方式极不合理，先“下载安装”而后才能“了解隐私政策”的顺序并不是“知情”而后“同意”的理想场景和方式。有学者考察了外国应用软件的运行后发现，“英文APP在应用平台搜索界面即可跳转查看隐私政策全文，方便用户在下载、安装、注册使用前，全面透明地了解APP各项内容，辨别是否下载使用此款APP”。[②]此种模式才是我们向往的。

此外，选择权的核心就在于选择“不”的能力，对此，经营者应当重视隐私政策的可读性，包括使用语言的通俗化、层次分明又重点突出的段落布局、需要获得授权之事项及范围的明确化等。《欧盟条例》第7条规定，用户的同意是基于充分知情的前提自由做出的，实践中通过“推定同意”方式获得用户同意将很难被认为是合法有效的，即“实践中普遍存在的通过冗长晦涩的隐私政策来获取用户同意，或者让用户在签订

① 程啸：《论大数据时代的个人数据权利》，《中国社会科学》2018年第3期。

② 刘娇、白净：《中外移动APP用户隐私保护文本比较研究》，《汕头大学学报》(人文社会科学版)2017年第3期。

业务协议时通过'打钩'方式作出一揽子授权的方式将失去合法性。业界普遍认为,《欧盟条例》关于有效合法同意的严格规定,使得用户的同意不会像现在这样被轻易获得"。①

(二)数据收集的程度问题:从"最大化"到"最小化"

2016 年 6 月,国家互联网信息办公室发布的《移动互联网应用程序信息服务管理规定》第 7 条规定,未向用户明示并经用户同意,不得开启收集地理位置、读取通讯录、使用摄像头、启用录音等功能,不得开启与服务无关的功能。然而前述中国消费者协会"APP 个人信息泄露情况"调查发现,手机应用软件存在过度采集个人信息的普遍趋势。以表 4 中的核心指标——设备权限调用——为例,"读取位置信息和访问联系人权限是安装和使用手机 APP 时遇到情况最多的,分别占 86.8%和 62.3%。此外,受访者被要求读取通话记录权限(47.5%)、读取短信记录权限(39.3%)、打开摄像头权限(39.3%)、话筒录音权限(24.6%)的比例也相对较高"。②如果说打开位置目的相对而言还多些的话,那么超过 60%的应用软件调用用户通讯录是为了什么?③ 显然,绝大多数应用软件调用通讯录的目的是在过度采集用户的个人信息。

无论是《欧盟条例》还是美国的公平信息实践原则,④都将"数据最小化"视为重要内容,并为之做了精心设计。例如,《美国儿童网络隐私保护法》为了纠正互联网企业对儿童个人信息的最大化收集和利用的默认规则,作出 4 项规定:(1)明确了具有法律效力的网站隐私声明必须包含的内容,其目的在于避免出现那种不容讨价还价的隐私声明和用户同意;(2)赋予父母一项权利,使他们有权获得网站向其子女收集的一切信息;(3)联邦贸易委员会可以通过解释来避免行业自律中出现最大化信息收集的规则;(4)严格限制商业网站将公开更多个人信息(超过合理、必要限度)作为儿童参与游戏、获得奖励或在该网站上进行其他活动的前提条件。⑤ 国外如此,国内亦然。除消费者协会持续关注应用软件非法收集用户个人信息外,2019 年 6 月 1 日,全国信息安全标准化技术委员会也发布了《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》(以下简称《指南》),对地图导航、网络约车、即时通讯社交、网络支付、网上购物等 16 类应用软件正常运行基本业务功能所需收集的必要信息予以明确,并对因"个性化推荐、提高用户体验和改善服务质量"而收集用户其他信息的情形单列了合规性审查要素,包括必要性判断、告知用户并征得同意、去标识化处理以及提供"退出"选项等。《指南》为落实《网络安全法》第 41 条网络经营者收集用户个人信息的原则而设,指向移动互联网应用中存在的超范围收集、强制授权、过度索权等问题,对规范移动互联网应用的信息收集具有重要意义。但遗憾的是,《指南》对网络经营者仅具参考价值,互联网企业会不会主动缩减收集、利用个人信息的范围,更大的可能是视其市场地位、利润及不良后果而定,《指南》能否发挥预期作用还未可知。但不管怎样,应用软件收集用户信息的目录体现在隐私政策文本之中,如果不能对隐私政策进行合规性审查,那么经营者会在隐私政策合规的光环下,对用户信息的收集变得更加肆无忌惮。

(三)数据留存期限问题:从"无统一规范"到"有生命周期"

阅读 49 例隐私政策文本发现,虽然有 61.2%的应用软件隐私政策中有数据留存条款,但是这些条款远谈不上规范,甚至可以说,对有些数据留存条款而言,用户停止使用或注销账号后,个人信息保存多长时间不受任何实质性限制。依据留存时间长短,时间节点有以下几种:账户注销后的 10 个工作日,1 个月,3 个月,6 个月,36 个月,5 年,等等。还有些规定则模糊不清,如微信、天猫、天天快报等应用软件的隐私政策规定个人信息的保留期限为实现目的所需的时间,至于这个所需时间到底为多久,无法轻易确定。

---

① 王融:《大数据时代:数据保护与流动规则》,人民邮电出版社 2017 年版,第 172 页。

② 中国消费者协会:《APP 个人信息泄漏情况调查报告》, http://www.cca.org.cn/jmxf/detail/28180.html,2018-08-29。

③ 在 49 款应用软件中,唯有网易新闻、百度地图和墨迹天气 3 款应用软件的隐私政策中有设备权限调用说明。一般来说,打开位置目的要么查找路线及导航,要么提供当地天气,要么判断登录账户是否安全及推荐周边功能场所,而调用通讯录的目的在于迅速为联系人充值、办理贷款等。

④ 公平信息实践原则是美国消费者隐私保护与个人信息保护监管中的重要原则。它源于美国健康、教育和福利部在 1973 年的开创性报告——《公民记录、计算机和权利》,是 1974 年《美国隐私法》的核心,也是美国隐私监管机构(美国联邦贸易委员会)执法活动的重要依据。该原则主要包括透明性、个人参与、明确用途、数据最小化、使用限制、数据质量和完整性、安全性、责任和审计等内容。

⑤ 转引自王融:《大数据时代:数据保护与流动规则》,人民邮电出版社 2017 年版,第 31 页。

数据有生命周期对于数字生态建设来说是必要的。有史以来,“记得”是例外,“遗忘”是常态。但随着数字技术的发展,“遗忘”成了例外,“记得”反成常态。欧盟曾基于反恐的需要,于2006年制定了《数据留存指令》(以下简称《指令》),并将数据留存期限界定在6—24个月。但是2014年4月8日,欧洲法院便裁定《指令》无效,原因在于,法院认识到,留存数据使得以下情形成为可能:“识别与用户或订户通过任何方式通讯的人的身份,识别通信时间以及通信发生的地点,了解用户或订户在一定时期内与特定的人的通信频率”,而指令“允许国家有关机构访问这些数据,是以一种非常严重的方式干涉了尊重私人生活以及保护个人数据的基本权利。进一步而言,留存数据以及在未通知用户或订户的情况下使用数据,可能使得相关人感觉个人生活受到持续监控”。[①]因此,有必要为数据使用者规定一个“到期日”,只要到期日来临,设备就自动删除相关数据。这种“到期日设计”源于数据保留原则中的“目的限制”,“如果是因为某特殊原因而需要将个人资料委托给某人,在目的实现之后,不再有允许使用该个人资料的条件,自然就该将个人资料删除”。[②]

除数据留存期限外,还需注意数据留存的地域。地域问题并不为大多数应用软件企业所重视,因此隐私政策中规定数据留存地域的并不多,少数有此规定的都简单地将留存地域设置为“境内”。但有无数据留存“境外”的情形呢?49例隐私政策中有两例典型:一是《陌陌隐私权政策》规定跨境直播或境外发布动态等行为时,数据可能存储在境外;二是《美图秀秀服务协议及隐私政策》规定当服务器在其他国家时,数据可能存储于国外。可见,数据存储境外的情形是有的,尤其是在境外使用该应用软件的情形下,此时数据存储地该如何规定?因此,数据留存并不仅仅是期限的问题,还有地域的问题。可惜的是,绝大多数应用软件隐私政策中都无相关的内容。

(四)数字广告推送问题:从“不请自来”到“拒收有门”

传统的以“客户概况分析”为基础的广告业正在悄然发生变化。“传统模式中,企业既能推销自己的产品和服务,同时消费者也没有过多地暴露隐私。在充斥着收音机、电视机和印刷广告的年代,信息流从企业自由地流到消费者那里,却几乎没有什么个人信息会被别人搜集。而在网络时代,每当消费者搜索某个产品或是浏览某个广告时,他的这些活动就会被迅速地记录到一份详细的个人档案中,而这种信息搜集过程完全是背着消费者进行的。”[③]显然,广告正在经历一个从传统印刷到智能手机广告推送的巨大转变。“不像个人电脑和电视,智能手机的天性就决定了它是一种个人设备,几乎总是为一个单一的、可识别的个人所拥有,这一特性为广告商们与客户建立更深的亲密关系提供了绝好的机会。大数据分析和移动广告的结合,奏响了市场营销的新乐章,这意味着广告从此可以与数百万潜在客户进行更亲密的、一对一的互动。”[④]广告模式的转变意味着应用软件经营者对消费者个人信息最大限度的商业利用,然而,问题在于,经营者基于“改善产品或改进服务的需要”或“个性化产品和服务的需要”有权通过邮件、短信、电话等形式发送广告,那么消费者有无权利拒绝这些“不请自来”的广告呢?答案显然是肯定的。没完没了的数字广告推送对公民“私人生活安宁”带来了侵扰,程度严重的就侵犯了公民的隐私权。因此,一项合规的隐私政策必须要保证消费者“拒绝”这些广告的权利。2003年《美国反垃圾邮件法》就要求企业或广告商必须保证用户有随时退订电子广告的自由,且必须在10个工作日内处理用户的退订请求,否则可处最高600万美元的罚款和5年监禁。[⑤] 可惜的是,在49例隐私政策中只有19例(占38.8%)有“广告推送及退出”的说明。并且,“退出”或者说“拒绝接收广告”的方式也比较单一,要么发送邮件,要么电话告知,都不能算是便捷高效的拒绝方式。这不得不说是一个巨大的遗憾。

(五)数据共享、披露、转移规则问题:从“模糊”到“清晰”

① 转引自王融:《大数据时代:数据保护与流动规则》,人民邮电出版社2017年版,第61~62页。
② 李延舜:《大数据时代信息隐私的保护问题研究》,《河南社会科学》2017年第4期。
③ [英]约翰·帕克:《全民监控:大数据时代的安全与隐私困境》,关立深译,金城出版社2015年版,第63页。
④ [美]达尔·尼夫:《数字经济2.0:引爆大数据生态红利》,大数据文摘翻译组译,中国人民大学出版社2018年版,第55~56页。
⑤ 参见薛敏芝:《美国新媒体广告规制研究》,《上海师范大学学报》(哲学社会科学版)2013年第5期。

“不同于物质性的东西,数据的价值不会随着它的使用而减少,而是可以不断地被处理。”[①]因此,尽管原则上消费者的个人数据不得共享、披露与转移,但在现实生活中,“个人信息收集和存储的简便,加上利用这些信息的超强能力,产生了巨大的商业压力,无法抵制能够产生附加价值的难以预料的二次使用的诱惑”。[②] 49 例应用软件的隐私政策均对消费者数据的共享、披露与转移进行了规定。但对隐私政策进行分析后发现,经营者多是在强调:有权与其关联方、合作伙伴(如物流方、支付方、第三方服务与供应商等)共享消费者数据;有权在企业发生合并、分立、清算等情形时,转移消费者数据;有权在数据主体同意、维护公共利益或他人合法利益、涉诉等情形时,合法披露相关数据。换句话讲,经营者强调自己的权利太多,而吝于承担相应的义务和责任。例如,在确需数据共享与转移时,是否应当先告知消费者处理数据的目的、所涉个人数据的范围、接收方类型以及应负的安全及其他法律责任等?只有权利条款而无义务或责任条款,是经营者面对消费者在数据收集和利用方面“强弱地位”的再次体现。

在数据共享、披露、转移规则改进的过程中还有两个特别值得注意的地方:一是对用户个人信息和个人敏感信息予以恰当分类,并作不同处理。有学者强调的“两头强化”就是指在个人敏感信息与一般信息区分的基础之上,通过强化个人敏感隐私信息的保护和强化个人一般信息的利用,调和个人信息保护与利用的需求冲突,实现利益平衡。[③] 美国学者韦克斯持相同的观点,认为隐私权所提供的保障应只限于某类别的资料,这些资料必须“是关于某个人的,而且可合理预期他会视为私人或敏感的资料,并因此而希望可以将其保密,或限制这些资料的收集、使用或流通”。[④]二是归属于同一企业的不同产品(应用软件)隐私政策允许共享用户数据的问题尤其值得关注。在 49 例隐私政策中就有此现象存在,如微信、QQ 阅读、QQ 音乐、腾讯视频、全民 K 歌的隐私政策与 QQ 的隐私政策之间的关系,彼此互为关联方,从而有权将各自用户的个人数据予以共享。这就是互联网巨头公司的数据聚合效应。外国的应用软件也有相同的情形,如谷歌公司早在 2012 年 3 月就抛弃此前 60 多种不同产品的不同隐私政策共存情形,整合用于所有服务中,包括谷歌、谷歌网络视频、谷歌邮箱等。这种隐私政策实现了不同产品线用户的数据互通,极大地增强了谷歌各种产品的综合竞争力。但问题在于,一方面,谷歌公司内部接触用户数据的频度增加,数据泄露的可能性与数据保护的难度也大大增加;另一方面,“新隐私政策允许 60 多种产品共享用户信息,实际上是将分散在 60 多种产品的用户隐私信息聚合,使用户在网上的形象更为立体、真实,用户的隐私也就受到极大侵犯”。[⑤]进一步讲,用户数据聚合使得应用软件企业对消费者的数据监控程度更加深化,“这些档案文件造成了消费者和提供必需服务的公司之间的信息不对称。因此,整个过程增强了公司的力量,而削减了消费者的自由”。[⑥]

(六)数据安全保护措施问题:从“敷衍”到“详列”

建立信息安全管理制度,并有完备、可行的信息安全保护措施是衡量一个企业数据保护能力的重要参考依据。在 49 例隐私政策中有 33 例提及信息安全保护或安全应急响应(占 67.3%)。这个数字有点小,并且在各项隐私政策中安保条款“肥瘦不一”,差异巨大,内容丰富者相关制度及保护措施篇幅可达两页,内容简略者仅仅述及“公司建有完善的信息安全管理制度,并有各项安全保护措施保障用户的数据安全”,再无其他。

一般来说,完善的信息安全管理制度起码应具备以下内容:(1)个人信息安全的技术保护。无论是用户数据的访问控制、加密套层传输加密技术还是高级加密标准 256 位加密或以上强度的加密算法、敏感信息脱敏技术等,都值得企业加大投入,技术安全保障程度越高,自然会吸引更多的用户青睐。(2)个人信息

① [英]维克托·迈尔一舍恩伯格、[英]肯尼思·库克耶:《大数据时代:生活、工作与思维的大变革》,盛杨燕、周涛译,浙江人民出版社 2013 年版,第 132 页。

② Joel Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 Stanford Law Review, 1315 (2000).

③ 参见张新宝:《从隐私到个人信息:利益再衡量的理论与制度安排》,《中国法学》2015 年第 3 期。

④ Raymond Wacks, Personal Information—privacy and the Law, Clarendon Press, 1993, p.26.

⑤ 方兴东、张静、刘国辉:《谷歌产品对用户个人隐私的影响——表现、趋势与对策》,《新闻界》2014 年第 11 期。

⑥ [美]理查德·斯皮内洛:《铁笼,还是乌托邦——网络空间的道德与法律》,李伦等译,北京大学出版社 2007 年第 2 版,第 147 页。

安全的人员配备。企业必须建立专门的数据保护团队，并对直接相关人员进行培训，岗位到人，责任到人。(3)个人信息安全事件的处置流程。企业应明确安全事件、安全漏洞的分类分级标准，并针对不同等级设置相应的事件处理流程。(4)个人信息安全应急预案。当发生大规模用户数据泄露、毁损或丢失时，应启动个人信息安全应急预案，对事故基本情况、可能影响、企业采取的紧急措施、补救措施、对数据主体的自助措施建议等，必须通过电话、短信、邮件、公告、推送等方式予以告知，并立即、主动向监管部门上报安全事件的处置情况。

四、应用软件隐私政策合规性贯彻落实的配套设计

智能互联时代，手机应用软件获取用户个人信息的范围和程度是前所未有的，而获取的越多，用户的信息安全和隐私问题就越严重。隐私政策既是互联网企业收集、存储、利用个人信息的说明，又是保障消费者数据隐私的社会承诺，必须让它发挥切实的作用，而不能让其仅作为互联网企业尊重用户隐私的自我标榜。如果说上部分探讨的是微观层面隐私政策具体条款改进的话，那么接下来就需要在宏观层面研究如何将隐私政策落到实处。

(一)克服集体行动难题

隐私政策的合规审查往往并不尽如人意。应用软件经营者常引用“买者自负”原则，声称用户自愿签署这种“浮士德式交易”，属于“私法自治”的范畴，国家无权干涉。然而，“私法自治作为一种形式上人人平等的自由，没有顾及实际上并非人人平等的事实。人与人之间在财产、体能和精神能力，在市场地位和掌握信息以及在其他许多方面，到处都存在着差异”。[①]人与人之间尚且如此，更何况用户与企业之间。对于消费者来说，勾选接受隐私政策并安装使用应用软件实属无奈之举，尤其是面对选择较少、市场化程度和规范程度都较低的应用软件时。然而，随着个人信息保护的呼声渐涨，公民的隐私意识增强，用户开始对应用软件隐私政策不满并进而寻求改变之时，集体行动的难题便产生了。

所谓集体行动，是指大家一起行动，共享行动的收益并共担行动的风险。所谓集体行动难题，是指面对侵犯集体中每一个成员利益的非法行为时(此时也可称社会公共利益受损)，反而少有人站出来为权利而斗争。擅长功利算计的个人发现：最好的行为是不作为，最好的策略是“围观”“坐等”，等待他人出头，然后自己“搭便车”。事实上，这一难题古已有之。早在2000多年前，亚里士多德就认识到：“凡是属于最多数人的公共事务，却常常受到最少人的照顾，人们关怀着自己的所有，而忽视公共事务；对于公共的一切，他至多只留心到其中和他个人有些相关的事物”。[②]美国公共选择理论大师奥尔森也在其著作中谈道：“除非一个集团中人数很少，或者除非存在强制或其他某些特殊手段以使个人按照他们的共同利益行事，有理性的、寻求自我利益的个人不会采取行动以实现他们共同的或集团的利益。”[③]换句话讲，即使个人都是有理性并寻求自我利益的，他们仍然不会自愿采取行动以实现共同的或集团的利益。面对历史和现实，必须承认：个体是自私的，个人能力也是有限的。但“皮之不存，毛将焉附”？“社会不可能像鸵鸟那样将脑袋扎进沙堆，然后假装什么都没发生或是那些有能力去收集和出售个人数据的组织会自觉地在将来自我约束，改做传统生意。”[④]必须采取措施来克服集体行动的难题，从而使隐私政策的合规性审查变得有意义。克服集体行动难题，需要从两个方面着手：一是实施激励机制，鼓励用户在发现应用软件隐私政策合规性存疑时，主动向消协、监管机关等有权部门投诉。虽然主张权利、抵御侵害是每一个权利主体的义务，但是在现实中，消费者与经营者力量的不对等、成本与收益的不平衡往往会消弭消费者采取行动的积极性。对此，奥尔森认为：“一个集体，一个社会，要建立合适的激励机制，奖励那些为共同利益作出贡献的个人，惩

① [德]迪特尔·梅迪库斯：《德国民法总论》，邵建东译，法律出版社2013年版，第144页。
② 转引自涂子沛：《大数据》，广西师范大学出版社2015年版，第150页。
③ [美]曼瑟尔·奥尔森：《集体行动的逻辑》，陈郁等译，上海三联书店2014年版，第2页。
④ [美]达尔·尼夫：《数字经济2.0：引爆大数据生态红利》，大数据文摘翻译组译，中国人民大学出版社2018年版，第188页。

罚那些没有承担集体行动成本的'搭便车者',从而营造关心公共利益的社会文化和运行机制。"[①]至于激励方式为何,可以是物质,也可以是荣誉,总归不能让"为己又为公"的消费者"跑了腿"还"寒了心"。除激励机制外,还有个可行的路径就是公益诉讼。关于这一点,我们可以从美国和韩国的相关制度中寻求借鉴。《美国金融服务现代化法》规定美国联邦贸易委员会可以提起诉讼,《美国儿童网络隐私保护法》也赋予国家检察官一项权力,使他们得以依据这部法律提起民事诉讼,从而使得国家检察官扮演了一个至关重要的角色。可见,美国的信息隐私权法往往依赖于民事诉讼以及个人采取的其他行动来调整信息保护实践和原则。[②]《韩国个人信息保护法》第 7 章第 51 条[③]则专门规定了个人信息团体诉讼制度,至于什么样的团体有诉讼资格,《韩国消费者基本法》第 29 条给出了答案:在公平交易委员会登记的,符合一定条件的团体有权提起团体诉讼。[④] 回到我国,在《中华人民共和国民事诉讼法》第 55 条以及《中华人民共和国消费者权益保护法》(以下简称《消费者权益保护法》)第 37 条规定公益诉讼制度的前提下,应明确消费者协会有权对应用软件隐私政策提请监管部门进行合规审查,以及对企业侵犯消费者个人信息权利的行为提起诉讼。至于消费者个人,如果其秉持为权利而斗争的理念,对应用软件隐私政策的合规性及侵权行为说"不"时,那么监管部门及人民法院也理应支持和受理。

(二)对应用软件隐私政策的问责

少数应用软件隐私政策中含有责任条款,但仔细研读发现,皆为免责条款(6.1%)。严格说来,这项统计并不十分精确,因为统计时排除了用户使用第三方服务的情形,而绝大多数应用软件隐私政策文本中皆有此类条款。但无论是旗帜鲜明的免责还是隐晦的免责,这些声明与隐私政策的合同及社会承诺属性截然背离——隐私政策绝不会因单向的"告知""勾选同意"就自动获得责任豁免。事实上,"告知与同意"原则在数据保护法中受到越来越多的质疑:一方面,"'通知与同意'的方式是实践中应用平台、程序或者网站服务要求个人明确同意对其个人数据信息收集使用的做法。但是只有在臆想的世界中用户才真正阅读这些通知的内容并在表明其同意之前真的理解其含义。'通知和同意'在服务者和用户之间形成了一个不平等的有关隐私的谈判平台。服务者提供了一个复杂的,要么同意要么离开的隐私条款,而实际上,用户仅仅有几秒钟的时间去评估它。这是一种市场失效"。[⑤]换句话讲,"告知与同意"这种低效的选择无法与大数据的高效处理相适应,因此个人不得通过一揽子同意来完全交付自己的个人信息。另一方面,"告知与同意"原则更多适用于个人信息的初次收集和利用,但大数据的价值更多源于它的二次(多次)利用,这就颠覆了当前隐私保护法中以个人为中心的思想。"在大数据时代,我们需要设立一个不一样的隐私保护模式,这个模式应该更着重于数据使用者为其行为承担责任,而不是将重心放在收集数据之初取得个人同意上。"[⑥]

美国政府一向主张制定隐私法的宗旨是防止滥用而不在于保护。2012 年 2 月 23 日,美国总统奥巴马作了名为《网络环境下消费者数据的隐私保护》的工作报告。该报告指出:"隐私的内涵不限于独处和私密。只有保护其免受个人信息滥用的滋扰,美国公民才能自由地从事商业活动、参与政治活动或者寻求医疗帮助。这是我们以法律手段保护金融和医疗信息隐私以及保护消费者个人信息免受不公平和欺骗性利用的原因。"[⑦]因此,"在法律和据以获得信息的合同约定中没有禁止性规定时,即使未经本人同意,信息的

① 转引自涂子沛:《大数据》,广西师范大学出版社 2015 年版,第 150 页。

② 参见[美]保罗·M·施瓦茨:《网络隐私权和国家》,廖嘉娴译,载张民安主编:《公开他人私人事务的隐私侵权》,中山大学出版社 2012 年版,第 506~508 页。

③ 《韩国个人信息保护法》第 51 条规定,属于下列各项的团体,在个人信息处理者拒绝进行集体纷争调解或不认可集体纷争调解结果的情形下,可以向法院提出请求禁止或停止权利侵害的诉讼。

④ 参见康贞花:《韩国〈个人信息保护法〉的主要特色及对中国的立法启示》,《延边大学学报》(社会科学版)2012 年第 4 期。

⑤ 吴伟光:《大数据技术下个人数据信息私权保护论批判》,《政治与法律》2016 年第 7 期。

⑥ [英]维克托·迈尔-舍恩伯格、[英]肯尼思·库克耶:《大数据时代:生活、工作与思维的大变革》,盛杨燕、周涛译,浙江人民出版社 2013 年版,第 220 页。

⑦ 周辉、孟兆平等:《网络环境下消费者数据的隐私保护——在全球数字经济背景下保护隐私和促进创新的政策框架》,《网络法律评论》2013 年第 1 期。

二次使用一般也被认为是合法的”。[①]而防止滥用最好的途径莫过于规定严格的法律责任，因为“数据使用者比任何人都明白他们想要如何利用数据。他们的评估（或者由他们所雇用的专家制定的评估）避免了商业机密的泄露。也许更为重要的是，数据使用者是数据二级应用的最大受益者，所以理所当然应该让他们对自己的行为负责”。[②]欧洲在问责制上持相同的观点，如欧米茄基金会的史蒂夫·赖特和宙斯基金会的专家们就一致建议欧洲议会，所有与数据库相关联的监控技术都必须置于一定的问责体系下施行。[③]

那么，应用软件隐私政策是否可以问责？又如何问责？已出台的《网络安全法》《消费者权益保护法》《电子商务法》皆规定了互联网企业的信息安全与隐私保障义务，此即对经营者进行问责的依据。至于所承担的责任类型，《消费者权益保护法》第29条、第50条及《中华人民共和国刑法修正案（九）》分别规定了经营者所应承担的民事责任、行政责任及刑事责任。可以说，制度层面的静态安排已没有问题，真正的问题在于如何问责。美国对隐私政策的执法主要依据两部法律，其中《美国公平信用报告法》对不公平及欺诈性商业行为规定了严格的责任（同样包括民事责任、行政责任及刑事责任），而责任的实现仰赖于《美国联邦贸易委员会法》。《美国联邦贸易委员会法》第5条规定委员会负有禁止市场不公平与欺诈性商业活动的职责。近几年来，美国联邦贸易委员会对该法第5条进行了充分的援引和解释，据以对公司隐私政策进行执法。在特定案件中，“被认为是具有误导性或欺骗性的行为包括错误的口头或书面表述，误导性的报价，未经充分披露而出售有风险或系统缺陷的产品，……未履行所承诺的服务，未实现担保义务”等，都被认为违反第5条规定。[④] 不仅如此，美国联邦贸易委员会还享有程序上的、调查的和强制执行的权力，保证责任的实现。与之相比，我国最大的问题在于缺乏这样一个强有力的专门机构，个人信息保护法缺失带来的不利影响不仅仅是立法层面的，还体现在执法上。市场监督管理部门面对此情形都力有未逮——它们一直从事传统行业的监管。唯有专门的数据保护机构，才能匹配相应的执法措施，让互联网企业真正承担起相应的数据保护责任。

（三）行政监管与公司治理、行业自治相结合

“用经济学的术语来说，隐私的丧失是一种市场失灵。”[⑤]数字经济虽然是一种新兴的、值得期待的经济样态，但是数字经济的健康、良性发展不能以牺牲公民的隐私为代价，数据收集与利用过程中的安全和隐私成本不能由数据主体来承担。围绕隐私政策凸显的合规审查，单靠市场显然无法矫正这个失灵，而需要做到3个方面：从设计着手隐私的公司治理、以标准化和认证为核心的行业自治以及能动、有效的行政监管。

首先，法律法规要促使企业承担更多的社会责任，隐私政策正是这一理念的体现和结晶。一方面，越来越多的消费者开始注意到隐私政策，对之阅读和审视，并进而希望借助隐私政策寻求个人信息的安全和隐私不受侵犯。而对于企业来讲，消费者的需求就是企业改进的方向。另一方面，互联网企业要正视隐私的价值，其隐私政策绝不仅是收集和利用消费者个人信息的说明以及获取消费者“同意”的路径，而应将隐私政策视为现代公司治理的重要组成部分。美国学者彼得·德鲁克曾说，大型企业有能力拥有“政策和专门制定政策的机构，使它们摆脱日常运营中的真实难题，从足够长远的角度看待问题，并考虑到组织与社会的关系”。[⑥]隐私政策问题涉及战略性议题而不仅是操作性问题，隐私政策应该与企业的战略决策及核心价值相契合。上至企业高层，中至企业隐私官，下至直接负责员工，都应重视企业隐私政策并视其为核

① ［美］理查德·C·托克音顿、［美］阿丽塔·L·艾伦：《美国隐私法：学说、判例与立法》，冯建妹等译，中国民主法制出版社2004年版，第209页。

② ［英］维克托·迈尔－舍恩伯格、［英］肯尼思·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社2013年版，第221页。

③ 参见［英］约翰·帕克：《全民监控：大数据时代的安全与隐私困境》，关立深译，金城出版社2015年版，第62页。

④ See Daniel.J. Solove&Woodrow Hartzog, the FTC and the New Common Law of Privacy, 114 Columbia Law Review, 583 (2014).

⑤ ［美］理查德·斯皮内洛：《铁笼，还是乌托邦——网络空间的道德与法律》，李伦等译，北京大学出版社2007年第2版，第144页。

⑥ 转引自［美］霍华德·R.鲍恩：《商人的社会责任》，肖红军等译，经济管理出版社2015年版，第83页。

心竞争力的一环。经济合作与发展组织于 20 世纪 90 年代就提出了“从设计着手隐私”的理念,认为“只有从一开始就按照隐私保护的需求设计和开发数据处理产品、程序和技术,才能使数据保护更加容易实施”。[①] 具体而言,企业的法律顾问或数据保护官应事前就参与到企业战略的制定决策中去,就像美国学者拉里·唐斯所言:“如果法律总顾问不参与公司制定战略性决策过程,那么这个企业就是在自寻烦恼;如果法律总顾问不知道什么是战略性决策——也就是说,如果根本没有在大体上了解该企业,那就更别提客户中的特殊业务了,麻烦可能已经来了”。[②]企业应通过隐私政策来彰显对消费者隐私的尊重,在个人信息的收集、使用过程中与消费者达成信任,从而赢得更多的市场份额。

其次,尽管我们对企业抱有希冀,但数据交易的回报和营销利润太高,使得我们又不能抱太高期望。这时候,行业自治不失为一种明智选择。有学者指出:“非官方手段在保护个人隐私方面往往更加高效、敏感。这一点在保护隐私权的具体例子中已得到证实——通过科技手段、市场、行业自律、企业竞争以及个人判断,人们可以获得相当周全的隐私权保护。”[③]一方面,行业自律可以改变当前互联网企业收集、利用消费者个人数据的“默认规则”,包括数据及数据库为企业财产、数据收集和利用最大化等。另一方面,数据挖掘与分析的先进技术对业内人士来讲并不陌生,就此而言,对消费者隐私危害最大的是市场,通过研发和制定规范来保障消费者隐私的也是市场。然而,行业自治的重要性不止于此,行业联盟可以通过制定隐私政策的范本对成员企业提供指引,我们可称之为“标准化”(模板)的隐私政策,并进而通过“认证”来标明某企业的隐私政策对消费者隐私的保护已经达到较高水平。这种认证“类似于一个隐私的‘绿色环保标志’,一方面促使企业向该标准看齐,另一方面又对已经达到该标准的企业贴标签,形成事实上的‘产品激励’机制”。[④]例如,美国的直销协会,就为其成员制定了隐私规则。这些规则要求在线公司发布并遵守隐私政策,告诉消费者他们的个人信息将被如何使用。直销协会有权批准具有遵守这些政策记录的网站,在线隐私联盟和网络广告促进会的公司联盟也制订了类似的标准。[⑤] 在 49 例隐私政策中,有 13 例(占比 26.5%)是明确告知消费者其信息安全系统是经过 ISO27001 权威认证的,这种认证无疑会增强消费者对企业数据保护的认同。

最后,如果将通过公司治理与行业自治来规范隐私政策的方式视为市场调节,那么还需要一个强大的外力来监督和促进隐私政策的贯彻落实。因为市场的天性是逐利,不可能将保护消费者隐私的美好愿望完全寄托于它本来的“潜在危害者”。这里体现的就是行政监管与业界的合作治理理念,各自发挥自己的优势,弥补对方天然的缺陷。以荷兰为例,“荷兰制定隐私保护法律以后,其实施都是先由各个行业协会提出企业行为规范,先后有银行、保险、直销等 20 多个行业提出了本行业的企业行为规范,以避免政府直接监管导致的信息不对称问题;然后,各个企业行为规范需要经政府批准后才能实施,以避免纯粹的行业自律机制可能导致的力度不够、运动员与裁判员不分现象”。[⑥]虽然行业规范是否要经过政府批准才生效在不同的国度也各有不同,但不能否认的是,能动、有效的行政监管对应用软件企业重视消费者隐私、制定较完善的隐私政策并进而贯彻、落实该隐私政策,是非常必要的。总的来说,世界范围内对隐私政策的监管模式分两种:一种是对应用软件经营者行为是否合乎企业隐私政策进行监管,如美国模式;另一种是对隐私政策本身是否合规进行监管,如欧盟模式。举例而言,美国木马智慧公司是一家网上销售幼教玩具的公司,其隐私政策曾做出如下令人放心的声明:“您可以放心,您的信息永远不会与第三方共享”。然而,2000 年 6 月该公司倒闭了,在破产程序中,木马智慧公司想出售它的消费者信息,因为根据美国破产法,这些信

① [英]维克托·迈尔-舍恩伯格、[英]肯尼思·库克耶:《大数据时代:生活、工作与思维的大变革》,盛杨燕、周涛译,浙江人民出版社 2013 年版,第 42 页。

② [美]拉里·唐斯:《颠覆定律:指数级增长时代的新规则》,刘睿译,浙江人民出版社 2014 年版,第 56 页。

③ 张民安主编:《公开他人私人事务的隐私侵权》,中山大学出版社 2012 年版,第 527 页。

④ 李延舜:《大数据时代信息隐私的保护问题研究》,《河南社会科学》2017 年第 4 期。

⑤ 参见[美]理查德·斯皮内洛:《铁笼,还是乌托邦——网络空间的道德与法律》,李伦等译,北京大学出版社 2007 年第 2 版,第 145 页。

⑥ 周汉华:《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,《法学研究》2018 年第 2 期。

息是可以用于清算的合法财产。后来,美国联邦贸易委员会起诉该公司违背隐私承诺出售消费者个人信息是不公平、欺诈的行为。[①] 换言之,美国联邦贸易委员会起诉木马智慧公司并不是因为其隐私政策本身违规,而是因为其行为违背了其自身的隐私政策,企业的隐私政策就是美国联邦贸易委员会执法的依据。2011年美国联邦贸易委员会起诉脸书公司欺骗消费者,其缘由也是脸书公司一系列行为并未遵守隐私政策中的承诺。欧盟则采用不同的监管模式,如谷歌公司于2012年采用新隐私政策的行为并未在美国受到处罚,但在欧洲,情况却非常严重,欧洲29个数据保护机构对谷歌公司展开了联合调查。据英国《卫报》报道,2013年12月19日,西班牙隐私监察委员会因谷歌公司违反该国个人数据保护法,对其处以90万欧元的罚款。原因是谷歌公司在未告知用户的情况下,将旗下不同在线服务的个人信息进行整合。据英国路透社报道,2014年1月8日,法国信息自由委员会称谷歌隐私新政策对个人隐私构成极大风险,用户根本不知道自己的哪些数据被搜集和使用从而对谷歌公司侵犯数据隐私权的行为处以15万欧元的罚款,而这是法国信息自由委员会有史以来作出的罚金最高的处罚。[②] 可见,欧洲诸国将监管的对象直接指向了企业的隐私政策,并对其合规性进行了审查,前述荷兰也是该种监管模式的典型。两种模式各有优劣,其背后是不同的数据保护理念:美国是以分散立法和行业自律为主的消费者隐私保护,而欧盟采用统一立法。至于我国对应用软件企业隐私政策如何监管,监管机构、监管职权、监管程序等如何设置,相信未来的个人信息保护法会有所安排。笔者倾向于采用上述第二种模式:一方面,要尊重隐私政策的存在,让其充分发挥作为企业与个人"沟通"的桥梁作用;另一方面,当私人组织行使私人权力(应用软件企业制定隐私政策)可能会威胁其他人的权利时,监管机关要予以限制。

总之,围绕隐私政策,企业、行业与政府之间应形成良性互动:一方面,"搭建跨界、包容的隐私保护共同体,使政府、企业和社会的隐私专业人员能够密切互动";[③]另一方面,强化监管及责任的承担,发现不合规的隐私政策,或者出现信息安全及隐私保护失败案例,要予以充分曝光,并严格追究其责任。唯有如此,多方联动,才能充分发挥隐私政策的社会功能。

五、结语

"并不是因为隐私让人感觉好或者对他们有好处,人们才需要隐私;相反,隐私对社会有好处是因为其能够推动个人的发展,而这些个人是民主社会的重要组成部分。"[④]数字经济的健康发展离不开消费者的隐私保护,而在此过程中,需要企业的积极参与。应用软件隐私政策绝不应是企业自我标榜的阅读文本,而是企业承担数据社会责任的具体体现,是消费者寻求隐私保护的信赖规范,也是监管部门重要的执法对象。可喜的是,绝大多数互联网企业已经认识到制定隐私政策的必要性并及时出台、更新隐私政策;遗憾的是,制定出来的部分隐私政策并不完善。以"核心指标+一般指标"作为评价标准,隐私政策条款存在诸多亟待改进之处。并且,要想将隐私政策落到实处,真正发挥其保障用户隐私的功用,还需要配套一些相关的制度设计。总之,构建以隐私政策为核心的企业数据合规,还任重而道远。

责任编辑　何　艳

① 参见汪靖:《不被洞察的权利——互联网精准广告与消费者隐私保护研究》,复旦大学出版社2016年版,第175页。
② 参见汪靖:《不被洞察的权利——互联网精准广告与消费者隐私保护研究》,复旦大学出版社2016年版,第186~187页。
③ 周汉华:《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,《法学研究》2018年第2期。
④ [英]文森特·米勒:《数字文化精粹》,宴青等译,清华大学出版社2017年版,第115页。