

Web 浏览器用户隐私安全政策问题与对策研究^{*}

何培育^{1,2} 马雅鑫¹ 涂 萌¹

(1. 重庆理工大学重庆知识产权学院 重庆 400054; 2. 西南政法大学博士后流动站 重庆 401120)

〔摘 要〕 为规范对网络用户个人信息的收集与使用行为, Web 浏览器提供商应遵循公开、透明原则, 制定完善的隐私政策, 以切实保护网络用户知情权与隐私权。文章基于实证考察, 对主要的七款 Web 浏览器的隐私政策从一般条款、信息收集与存储条款、信息使用与共享条款等方面进行比较研究。研究发现, 各 Web 浏览器的隐私政策在隐私保护水平、主要条款内容、权利与义务关系等方面存在问题, 应当以《信息安全技术个人信息安全规范》为指导, 从隐私政策条款的制定与程序的监督方面入手, 寻求解决路径。

〔关键词〕 Web 浏览器 隐私政策 隐私安全 个人信息

〔中图法分类号〕 D923; G201

〔引用本文格式〕 何培育, 马雅鑫, 涂萌. Web 浏览器用户隐私安全政策问题与对策研究 [J]. 图书馆, 2019 (2): 019—026.

2017 年 12 月 29 日, 由全国信息安全标准化技术委员会制定的《信息安全技术个人信息安全规范》(GB/T 35273-2017) (以下简称《个人信息安全规范》) 正式发布, 并于 2018 年 5 月 1 日起正式实施。Web 浏览器作为数据时代网络用户收集信息的基本工具, 存在隐私泄露的重大风险。Web 浏览器提供商发布的隐私政策是其遵循公开透明原则的重要体现, 也是约束自身行为和配合监督管理的重要机制。但 Web 浏览器的隐私政策在制定、实施、管理等方面还存在较多的问题^[1], 网络用户的隐私保护工作仍任重道远。基于此, 笔者对主流七款 Web 浏览器的隐私政策条款进行比较研究, 对照《个人信息安全规范》相关条款发现它们的问题与不足, 进而对 Web 浏览器提供商完善相关隐私政策提供建议。

1 文献回顾

1.1 Web 浏览器的隐私安全风险与防控机制

1.1.1 Web 浏览器的隐私安全风险

Web 浏览器是一个软件程序, 用于与 WWW 建立联

结, 并与之进行通信^[2], 它通过 URL 和超级链接来获取并显示信息资源的位置, 将多种网页集合、编排, 对 HTML 文件进行解释, 将多媒体信息显示出来, 以供用户浏览。

何培育^[3]、刘焕成^[4]、宋鹏等^[5]认为, 在个人信息收集过程中, 网络环境下的隐私安全风险主要表现为个人信息的过度 and 非法收集、黑客攻击与病毒入侵。武敏^[6]更进一步指出, 在个人信息收集过程中的隐私风险来源还包括技术的弱点和漏洞、执法需要和立法冲突。胡水晶^[7]也认为技术和政府的不可抗力是个人隐私的潜在威胁。同样地, 刘小霞、陈秋月^[8]从网络搜索技术出发, 认为技术本身是中性的, 但滥用积聚会带来个人信息安全风险, 表现为个人网络、现实行为被“监视”。

在个人信息使用过程中, 有学者^[3]认为网络隐私安全风险主要表现为网络经营者对个人信息的二次加工、出售或交换以及网络信息中介公司对个人信息专门的收集与分析服务。Smith 等^[9]也持同样观点, 指出企业在处理数据的过程中造成隐私泄露问题有 4 个相关的数据维: 信息的收集、误用、二次使用以及未授权访问。张军等^[10]将网络个人信息分为个人数据、数字行为和通信内容。姜明芳^[11]

^{*} 本文系 2016 年国家社科基金项目“大数据时代个人信息盗窃的法律问题与对策研究”(项目编号: 16CFX027) 和 2015 年重庆市博士后科研特别资助项目“大数据时代个人数据盗窃行为法律规制研究”(项目编号: Xm2015043) 成果之一。

指出隐私风险表现为边信息、定位和位置服务过程中的位置隐私泄露风险,数据隐私风险,身份隐私风险。

综合上述文献对网络隐私保护进行的研究,网络用户隐私安全风险主要体现于以下三个方面:第一,对个人信息过度、非法收集,即未经许可或超过许可范围的收集,如黑客入侵计算机系统窃取个人信息;第二,对个人信息过度、非法使用,即超过了法律规定或与当事人约定的适用范围,如非法出售个人信息;第三,信息主体的自我披露,网络用户由于疏忽大意,在网上留下了大量的个人隐私信息。

1.1.2 Web 浏览器隐私安全风险的防控机制

当前我国主要通过立法、技术、行业自律、政府监管、加强自我保护等措施防范与处理隐私风险,文章主要围绕立法和行业自律两个措施进行分析。

首先,从立法角度而言,曾诚等^[12]、段绩伟^[13]提出应当将网络隐私权作为一项独立的人格权;学习和借鉴其他国家对于隐私权成功保护的立法经验,适时制定我国个人隐私数据保护法。对此,刘焕成^[4]认为在明确的立法和修法之前,国家有关部门可以先制定隐私权保护的行政规章。在立法的具体内容上,梁志文^[14]提出不同数据应分别立法的原则,即对个人敏感数据实施特殊保护。赵文龙等^[15]也指出“特定的个人基本信息未经允许不得擅自收集”这一原则应在立法中予以确认。胡水晶^[7]认为可以构建数据存储、访问和处理的标准并强制执行确保个人数据的控制权和知情同意权,明确侵犯个人隐私的赔偿标准。李雨明等^[16]在梳理现行法律的基础上,提出了要明确用户对数据的所有权、控制权、处置权和知情权。

其次,从行业自律角度来看,行业自律措施主要包括适用于整个互联网行业的自律以及各个网络运营者的自律。刘焕成^[4]提出应当成立个人隐私保护协会,统筹规划网络隐私保护工作,同时制定具体政策;由工业和信息化部(以下简称工信部)和个人隐私保护协会联合成立网络隐私达标认证机构,负责审计、监督和检查各网络运营者对用户隐私权的保护情况;各网络运营者应加强隐私政策的制定,并做出详细解释。李延舜^[17]认为行业自律能将信息隐私保护具体化和标准化。武敏^[6]也指出网络服务商应制定和公布其隐私权政策,并与用户签订隐私安全协议。但华海英、孟晓明^[18]认为隐私政策的内容和执行上存在未能较好且公平的体现现行法规的要求等问题,而开展第三方网络隐私认证信息服务将会提供一个较好的市场环境。董燕影等^[19]、徐敬宏^[20]提出网络隐私第三方认证在保护个人隐私方面仍然存在不少障

碍,它应与法律保护相结合,同时加强政府对行业自律行为的监管。

基于现有的研究成果,笔者认为在当前对网络用户个人隐私保护立法不够完善的情况下,行业自律不失为一种可行且有效的保护措施。在行业自律的各个具体措施中,设置完善的隐私政策尤为重要。

1.2 隐私政策的法律性质和意义

1.2.1 隐私政策的概念与法律性质

网络隐私保护政策,是指网络运营者通过告知用户其个人信息可能被搜集、使用、与第三方共享的情况,以及自身使用个人信息时的免责条款,来告知网络用户在使用本网络服务时的信息安全问题,以达到与用户之间隐私保护的共识^[21]。隐私政策是网络运营者在其经营服务过程中,对用户个人信息合法收集、使用、保护的一种行业自律措施之一。

林旭霞^[22]认为网络用户协议是网络运营商单方拟定的与网络用户建立的合同,对于网络用户协议之外的“政策”“声明”,如隐私政策,只有在不违反《消费者权益保护法》第26条和《合同法》第40条中对格式条款的相关规定时,才可以认定其属于有效条款。段绩伟^[13]也认为网络运营者的隐私权政策声明是网络运营者与用户签订的关于个人资料利用及隐私权保护的合同,如若违反,则用户可依法要求运营者承担相应的法律责任。谈咏梅等^[23]认为单纯的网页浏览不会形成合同关系,只有当存在服务内容且用户同意(通过注册)才会形成网络服务合同。

笔者认为当隐私政策涉及一定的网络服务内容时,且在用户享受该网络服务前,网络运营者采取了征得用户同意的手段,则表示网络用户与网络运营者达成了协议,隐私政策则属于合同性质;或者当提及该隐私政策属于前述网络服务协议(合同)的一部分时,也属于合同性质。否则隐私政策只属于规范,不具有法律上的约束力。我国目前主要有《合同法》《消费者权益保护法》《电子签名法》等法律对此加以规范。

1.2.2 隐私政策的意义

为了消除公众的顾虑,网络运营者通过制定隐私保护政策,告知网络用户其会如何收集、使用个人信息,来证明其提供的产品或服务是安全的。

分析现有文献对隐私政策意义的研究,李延舜^[17]认为就目前来看,隐私政策确定的一些具体的权利和义务内容,能有效填补法律的空白地带,成为事实上的隐私保护规范。徐敬宏^[24]在考察隐私政策功能时发现,基于隐私政策的自

律模式是较为宽松的措施，网络运营者在行业协会的监督下，通过自我规范、自我约束，使得其在促进用户个人信息合理流动的同时又保证安全使用。魏来等^[25]认为在保护用户隐私上，隐私政策应是达到最低标准的；其除了能更好的提供保护外，也向用户提供规范的服务；维护了本行业和企业利益，避免恶性竞争，维护互联网持续健康的发展。

通过上述文献回顾可总结出，隐私政策对于不同主体都具有重要作用。对信息主体来说，隐私政策是网络运营者对其个人信息保护的承诺，信息主体可以依据该内容寻求保护，保障其合法权益。对于网络运营者而言，隐私政策通过告知用户其网络服务在何种情况下会收集用户信息、收集用户信息的目的和方式、免责事项等，提高用户的隐私信任倾向，进而通过影响用户的信任，对用户信息隐私意愿产生积极作用，使得网络运营者提供更好的产品或服务，进一步提高声誉^[26]。从社会层面来看，基于隐私政策的隐私保护工作能最大限度地给予网络运营者自我发展的空间，促进互联网和相关服务业快速、健康发展。

2 七款 Web 浏览器国内隐私政策内容对比分析

2.1 研究方法

文章选取了我国当前使用最为普遍的七款浏览器：百度浏览器、遨游浏览器、360 安全浏览器、猎豹浏览器、UC 浏览器、火狐浏览器、Internet Explorer（IE 浏览器）。下文将梳理七款 Web 浏览器隐私政策的具体内容并进行对比分析，从而发现各自在条款设置上的优点和不足。隐私政策是用户判断其个人信息是否被网络运营者保护的最直接依据。一般情况下，隐私政策的内容主要分为以下三个主要方面：①一般条例；②收集与存储用户个人信息；③使用与共享用户个人信息。下文就这三方面分别分析七款浏览器的隐私政策内容。

2.2 一般条例的对比

七款浏览器隐私政策的一般条例对比大致分为两方面：一般情况和责任部分（见表 1）。其中，一般情况包括首页链接次数、文件名称、最新更新时间和未成年人隐私保护说明。责任部分包括责任承担、免责声明、专门的联系方式和修订通知。

表 1 各个浏览器隐私政策一般条例的对比

浏览器	首页链接次数	文件名称	最新更新 时间	未 成 年 人 隐 私 保 护 说 明	责 任 承 担	免 责 声 明	专 门 联 系 方 式	修 订 通 知
百度浏览器	2	隐私权保护 声明	无	√	√			√
遨游浏览器	2	隐私策略	无		√			√
360 安全 浏览器	2	隐私保护 说明	2014-06		√		√	√
猎豹浏览器	2	隐私策略	2017-07	√	√			√
UC 浏览器	3	隐私保护 声明	2012-05		√	√	√	√
火狐浏览器	1	Privacy Notice	2017-09	√	√		√	√
IE 浏览器	4	隐私声明	2018-02	√	√	√	√	√

（注：访问日期至 2018 年 3 月 17 日；“√”表示提及，空白表示隐私政策里未提及。）

2.2.1 一般情况

其一，首页链接次数。在调查的七款浏览器隐私政策中，有六款隐私政策需要经过两次以上的首页链接才能查找到相应的隐私政策。其中特殊的是 UC 浏览器隐私政策的位置，它需要通过首页的“招聘”“走进 UC”两个条目链接，才可以看到“隐私保护声明”。其二，文件呈现方式。这七款浏览器的隐私政策都是以文本罗列的形式呈现，值得注意的是，IE 浏览器提供了下拉式的方式辅助阅读和浏览。其三，未成年人隐私保护的说明。在被调查的七款浏览器中，百度、猎豹、火狐与 IE 四款浏览器的隐私政策中设有专门针对未成年人隐私保护的声明。从年龄范围看，猎豹、火狐与 IE 浏览器针对的是 13 岁以下的未成年人，百度浏览器针对的是 18 岁以下的未成年人。但在《个人信息安全规范》中明确指出对未成年人的年龄限制为 14 岁。其余三款浏览器也均指出其不希望接受未成年人的个人信息，而且不会主动向注册用户中的未成年人提供基于兴趣的广告。

2.2.2 隐私保护责任条款

其一，责任承担和免责声明。从表 1 可以看出，UC 浏览器在隐私政策里设有专门的免责声明部分，而且内容较为全面。其他浏览器都将其网络服务协议中的免责声明适用于隐私保护，如百度在“使用百度前必读”里包含有适用所有百度产品的免责声明。其二，专门的联系方式。有四款浏览器在隐私政策的末尾直接提供了专门的联系方式，以便用户对隐私政策提出反馈。但是联系方式大多为邮箱和

服务网站,其中IE浏览器提供的联系方式最为全面,包括服务网站链接、数据保护专员、地址和电话以及专门的数据保护代表团队。其三,修订通知。有六款浏览器明确指出必要时会进行隐私政策的更改,保留了修订隐私政策条款的权利。360安全浏览器的隐私政策虽然没有专门的修订通知部分,但是其序言有关于隐私政策修改的文字说明。此外,猎豹对修订通知给予了用户十五天的异议期限。

2.3 收集、存储用户个人信息的对比

关于收集、存储用户个人信息的条款是网络服务隐私政策的重要内容,也是用户关注的焦点。七款浏览器对用户个人信息的收集与存储情况对比见表2。

表2 各个浏览器收集、存储用户个人信息情况的对比

浏览器	收集信息的目的	收集信息的内容	用户的权利	Cookie的说明			保存时限
				是否使用	自动安装	使用目的	
百度浏览器	√	√	√	√	√	√	
遨游浏览器	√	√	√	√		√	
360安全浏览器	√	√	√	√			
猎豹浏览器	√	√	√	√	√	√	
UC浏览器	√	√	√	√		√	
火狐浏览器	√	√	√				√
IE浏览器	√	√	√	√	√	√	√

(注:“√”表示提及,空白表示隐私政策里未提及。)

2.3.1 收集信息的目的、内容

七款浏览器的隐私政策均包含有关于收集用户个人信息的内容和目的,并说明了收集用户个人信息的途径。七款浏览器都声明了收集用户个人信息是“为了向所有用户提供更好的服务”这一目的。

收集个人信息的内容既包括非个人识别信息,如浏览页面内容、链接地址、访问日期和时间等,也包括个人识别信息。当然,各个浏览器的隐私政策声明了只有在特定条件下才会收集用户的个人识别信息,即满足收集个人信息的最小化要求。如百度浏览器的隐私权保护政策声明“我们可能会收集关于您使用产品和/或服务(包括使用方式)过程中的信息,此类信息包括设备信息、日志信息、位置信息等”,同时特别强调了这些数据信息都采用匿名的方式,并且会对信息采取加密处理,保证信息的安全性。具体来看,所收集信息的内容主要分为以下三类:用户主动提供的信息、用户在使用产品或服务过程中被收集的信息和来自第三方的信息。这在猎豹、火狐、UC、百度浏览器的隐

私政策里均有体现。

2.3.2 关于Cookie的告知

如表2所示,关于Cookie的说明在百度、猎豹和IE浏览器的隐私政策里体现得较完整。三者均提到使用Cookie将便于用户使用其产品或服务,帮助统计独立访客数量等。此外百度、猎豹和IE浏览器也告知了用户可以通过浏览器“设置”拒绝Cookie,但同时也强调了拒绝Cookie的后果。相比之下,对于未提及Cookie技术的,其隐私政策里没有声明不代表不使用,这样带给用户的隐私安全隐患反而更大。

2.3.3 用户权利声明

Web浏览器提供商不仅通过隐私政策里提及的技术措施保护用户个人信息,而且也赋予用户一些权利进行保护。这些权利虽没有被明确提出,但体现在隐私政策的具体条款里。这七款浏览器均对收集信息的内容进行了详细说明,告知用户哪些信息将被收集和使用,这是赋予用户知情权的表现;均允许用户对某些服务或者收集信息的行为拥有选择处理其信息的权利,如UC指出“您选择同意才会共享任何敏感的个人敏感信息”,这是给予用户选择同意的权利。

2.4 使用、共享用户个人信息权限的对比

隐私政策可被视为网络运营者对用户个人信息保护的一种承诺,因此,网络运营者有义务对收集的个人信息的使用情况进行说明。现将七款浏览器对用户个人信息的使用与共享情况对比,内容如下(见表3)。

表3 各个浏览器使用、共享用户个人信息的情况

浏览器	如何使用	何种情况下共享	和谁分享			破产出售的隐私保护	信息安全
			附属机构	第三方	其他第三方		
百度浏览器	√	√	√	√	√	√	√
遨游浏览器	√	√		√			
360安全浏览器	√						√
猎豹浏览器	√	√	√	√	√	√	
UC浏览器	√	√	√	√	√	√	√
火狐浏览器	√	√				√	√
IE浏览器	√	√	√	√	√	√	√

(注:“√”表示提及发生,空白表示隐私政策未提及或提及不会发生。)

2.4.1 个人信息的使用

如表3所示,这七款浏览器提供商均在隐私政策里说明了收集到的用户个人信息的用途。无一例外,有一个用

途高度一致,就是利用收集的用户个人信息提供、维护、保护和改进其产品或服务,同时可能会开发新的功能以提供用户使用。但同时,百度、猎豹、UC 与 IE 四款浏览器的隐私政策里也写明了其还可能将该信息用于发送促销信息和显示广告等商业目的。而且,百度浏览器和 UC 浏览器还提及另一个用途:保存用户与该浏览器联系时的通信记录,以便解决该用户遇到的任何问题,而且主动向用户发送有关产品或服务的重要通知。百度还提出了当提供个性化服务或保障合法权益时,如进行身份验证,将会使用用户的个人信息。

2.4.2 个人信息的共享

除 360 安全浏览器外,其余六款浏览器的隐私政策均对在何种情况下该浏览器提供商将共享用户个人信息进行了说明,也提示用户对于通过该浏览器链接到的其他公司的网站或产品,需要仔细阅读网站或产品本身的隐私政策,其不对任何第三方不当使用或披露用户信息的行为承担法律责任。如百度明确提出“以高度的勤勉义务对待您的信息”,但是也提出了在三点例外情况下,可能会向第三方提供用户个人信息。UC 与 IE 也采用同样的方法。火狐说明“只有当我们真诚地相信这是保护您、其他用户、Mozilla 或公众的权利、财产或安全的合理必要手段时,我们才会以这种方式共享您的信息”,而且会在信息风险暴露率降到最低后进行共享。遨游指出除与合作伙伴共享统计信息外不会将个人信息公开给其他第三方。

2.4.3 信息安全性

在七款浏览器隐私政策中,百度、360、火狐与 IE 四款浏览器在其隐私政策里设有专门的信息安全性的部分,明确指出会保护用户个人信息安全,并将使用各种安全技术和手段帮助保护其收集的用户个人信息,使其免遭未经授权访问、泄露或篡改。并且百度也在表明“您使用我们的产品和/或服务时所用的系统和通讯网络,有可能因超出我们控制能力之外的其他因素而出现安全问题”后,向用户推荐其 passport.baidu.com 的密保工具服务进一步保障用户信息安全。360、火狐和 IE 采用列举的方式介绍其为确保信息安全所采用的技术措施。如,IE 提出“当我们在 Internet 上传送高度机密的数据(例如信用卡号或密码)时,我们使用加密技术来保护这些信息的安全。”

2.5 总体对比结果

可将七款浏览器隐私政策各个方面的具体内容总结为以下三点:

其一,有关隐私条款的检索路径较为复杂,用户无法

较快速的找到隐私保护政策,且当更新其隐私政策时,往往不会及时通知用户。首先,文章调查的七款浏览器均设有隐私政策,可以认为是符合《网络安全法》要求的网络运营者应建立用户信息保护制度以及《个人信息安全规范》要求个人信息控制者应制定隐私政策的规定,但是在具体内容的设置上仍存在不完善之处,例如,大多数是在“关于”产品的类目下,而且位于首页最底部小字部分。这些使得用户在查找隐私政策时不够快捷,在阅读时较为不便,该做法不免让用户认为该浏览器提供商故意淡化其隐私保护责任。其次,一些浏览器提供商在其隐私政策里保留了单方、无条件修订隐私政策内容的权利,也写明了会通过合适的方式进行发布、通知,如 UC 表明“如果您继续选择使用我们的服务即表示您同意接受这些修改”。

其二,隐私政策对收集与存储用户个人信息的目的和范围以及如何使用 Cookie 等技术说明不清。网络运营者收集个人信息时应确保其合法性,对于间接获取的个人信息也应对其来源进行确认。根据《网络安全法》第 40 条、41 条,网络运营者应明示收集个人信息的目的、方式和范围,并获得被收集者同意。在七款浏览器中,首先,都指出收集用户个人信息的目的,采用“为了……,我们会收集和使用您的信息,本声明解释了收集和使用用户个人信息的情况”的句式简要说明收集用户个人信息的目的。其次,有超过半数的隐私政策缺乏专门对收集用户个人信息方式的说明,如 UC 浏览器的隐私政策仅仅在用户体验计划里提到“用户本地终端的数据缓存(Cookie)以及用户个人文件及隐私数据。我们会依据收集到的数据,汇总分析用于改进我们的产品”。

其三,大多数 Web 浏览器隐私政策未能明确告知用户所享有的权利以及浏览器提供商的义务。隐私政策的作用之一就是明确网络用户在使用网络运营者提供的服务或产品时所享有的权利。经前述对比可以发现,这七款浏览器均保障了用户的知情权,但对于其他权利的保护则稍有不足。《网络安全法》第 43 条和《侵权责任法》第 36 条均规定个人发现网络运营者有违反法律或约定的行为,有权要求网络运营者采取删除等必要措施,这赋予了用户对其个人信息的控制权,并有权要求予以删除,而在文章调查的七款浏览器中未明确体现。百度规定当用户注册信息有误时“我们会努力提供各种方式来让您快速更新或删除帐户内信息”。此外,《网络安全法》第 42 条和《消费者权益保护法》第 29 条都规定网络运营者在发生或者可能发生信息泄露、丢失的情况时,应当立即采取补救措施,这一条款即是赋予了网络运营者的安全保障义务,而在这

七款浏览器的隐私政策均未清晰地体现此义务的具体实施措施。

3 对 Web 浏览器隐私政策的完善建议

在网络活动中,隐私政策已随处可见。而我国现有的隐私政策在制定、实施、管理等各方面还存在较多的问题,网络环境下基于隐私政策的隐私保护工作仍任重道远^{[1]135}。文章认为,在形式上,隐私政策应设置在其首页比较突出的位置。在内容上,隐私政策应丰富、灵活。此外,应加强隐私政策的制定和监督,落实网络运营者法律义务的承担。

3.1 不断优化 Web 浏览器隐私政策条款设计

现阶段,网络运营者可从收集、使用信息两个过程着手,同时参考个人信息安全的基本原则以及《个人信息安全规范》的隐私政策模板与编写要求,制定较为完善的隐私政策,最终得以保护用户个人信息。例如,美国的网络用户隐私权利法案为保护用户隐私设定了7项原则;我国首个个人信息保护国家标准《信息安全技术、公共及商用服务信息系统个人信息保护指南》(GB/Z 28828-2012)中规定了个人信息管理者对个人信息处理的基本原则;《个人信息安全规范》规定了有权处理个人信息的个人信息控制者在处理个人信息时应遵循的基本原则,虽然该规范只是一项推荐使用国家标准,但其对个人信息的使用和处理做出了明确规定,对保护公民个人信息具有重要意义。在内容设计上,隐私政策条款主要包括但不限于以下四方面。

其一,隐私政策至少需要包含如下内容:网络运营者的基本情况;遵守法律规定的承诺;对用户个人信息的收集与存储、使用与共享、披露、安全的条款;Cookie的使用条款;关于特殊主体的信息保护;免责声明;相关责任的声明;纠纷解决机制;专门联系方式;内容修订事项;生效日期。

其二,关于用户个人信息的收集与存储条款,具体包括:收集与存储用户个人信息的目的及其合法性、对应的业务功能和留存时限;用户提供个人信息可能出现的风险、拒绝提供其个人信息时可能出现的后果;并且要提前征得用户授权同意,个人敏感信息适用明示同意;收集个人信息的方式,如关于Cookie技术的说明;具体保护用户个人信息安全、完整的措施说明,包括技术措施和其他必要措施,如当发生或可能发生个人信息披露、篡改、损毁时的应对机制。

其三,关于用户个人信息的使用与共享、披露、安全的

条款,具体包括:网络运营者使用与共享用户个人信息的目的及对应的具体内容;明确网络运营者主体不得披露、篡改、损毁其收集的个人信息,未经用户同意不得出售或非法向他人提供个人信息;允许用户自主控制个人信息收集,可以进行更正、删除等操作;关于出售用户个人信息的内容。

其四,网络运营者制定隐私政策时,还可以根据自身提供网络产品或服务的实际情况增添内容,即针对其产品或服务的特性强调某方面的隐私权保护,例如360安全浏览器的隐私保护说明特别强调其安全性。北京奇虎科技有限公司提倡360安全浏览器的服务价值是“给网民提供一个安全顺畅的上网环境”,在其隐私保护说明中,不仅设置有专门的关于个人信息收集的部分,而且在介绍了具有特色的“云安全”功能后,分别针对某一具体功能,如网银云安全、下载云安全等,设置了关于该功能的用户个人信息收集、使用条款。又如,在介绍网银云安全功能时提出为保障网银环境安全,将会读取用户的网银控件相关的注册表以及文件信息,但在介绍其他功能时,明确说明不会收集与用户个人身份相关联的信息。

3.2 加强 Web 浏览器隐私政策的合法性监督

在大数据时代背景下,用户个人信息也成为企业的重要资源,其掌握的个人信息具有很高的商业价值。对于盈利性企业来说,其制定的隐私政策作为辅助政策,尽量免除自己的责任才是其理性选择^[27]。因此,隐私政策的制定和落实无法单纯依靠企业自觉性,需要政府和第三方的监督,并且应当提倡和鼓励网络运营者加强行业自律,依照法律和行业惯例制定隐私权保护政策^[13]。

其一,明确相关政府管理机构的职责。如电信管理机构(包括工信部和各省、自治区、直辖市通信管理局)依法负责个人信息保护工作的实施、监督与管理。其二,充分发挥中国互联网协会的作用,可在个人信息安全基本原则的指引下,指导会员完善隐私政策设置,加强自律管理。其三,建议由工信部主要承担软件和信息服务业行业管理工作的信软司,其下设的信息服务业处提供网络隐私认证信息服务,负责评估和认证网络运营者的隐私保护状况,并进行监督和检查,给与达标标记表示授权认证。

虽尚未出现全国性的网络隐私保护的认证体系,但第三方测评机构提供认证服务在国内外已得到较为成熟的实践。国外较为成熟的是美国的TRUSTe和可靠认证计划(Reliability Seal Program)^[19]。我国《大连软件及信息服务业个人信息保护规范》(DB21/T1628-2012)是经历了日本

软件业的冲击后,由大连软件行业协会制定的大连地方标准,并为此建立了软件及信息服务业的个人信息保护认证体系 PIPA (Personal Information Protection Assessment) 办公室^[28]。该适用于大连软件产品的信息保护评价制度已形成较为成熟的评价、监督和认证机制,网络隐私认证机制也可以借鉴其进行制定和实施。

3.3 落实 Web 浏览器隐私政策违法行为的法律责任

信息安全保障工作需要技术、管理和法律等诸多方面的协调,涉及政府、企业等多方参与主体。国外已经将公司内部管理作为保障信息安全的重点^[29]。文章认为需要从公司和政府角度,落实其法律义务与责任。

3.3.1 明确网络运营者保护用户个人信息的义务

隐私政策的作用之一是规范网络运营者的法律义务与责任,但出于利益的考虑,网络运营者通常会增强对用户个人信息的控制权,弱化其保护用户信息的义务以规避责任的承担。近年来,我国立法机关越来越重视这一问题,并通过法律规定了网络运营者的信息网络安全管理义务和法律责任。

网络运营者应履行网络安全保护义务。具体解释为,提供网络产品或服务的网络运营者在合理限度的范围内负有保护用户个人信息和财产安全的义务。尤其当网络交易平台提供的产品或服务有偿时,其安全保障义务更为严格。其次,网络运营者也负有删除义务。《侵权责任法》第 36 条和《网络安全法》第 43 条都规定了网络服务提供者收到用户侵权通知后,应及时采取必要措施,予以删除。《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》对侵权责任法第 36 条进行了详细的解释,为该条款的具体适用做出了规定,以更好的规范网络违法行为。网络运营者若违反上述法律规定,承担的责任主要包括警告、没收违法所得、处违法所得一倍以上十倍以下罚款,最高可处一百万罚款;情节严重的,可吊销相关业务许可证;《中华人民共和国刑法修正案(九)》(以下简称《刑法修正案(九)》)在刑法第 286 条后新增了四种违反信息网络安全管理义务的严重情节,可处三年以下有期徒刑、拘役或者管制,并处或者单处罚金。

3.3.2 畅通 Web 浏览器隐私政策违法行为的救济渠道

其一,企业内部设立专职的个人信息保护责任人,建立申诉管理机制。这也是《个人信息安全规范》所明确要求的。根据前文分析,微软针对用户的隐私担忧和投诉等

问题,内部设置首席隐私官/数据保护专员,其主要通过 Web 表单连接用户,同时也提供了联系电话和邮件等方式。

国内网络运营者可以适当借鉴微软的做法,在其企业内部设隐私专员岗位,专门负责处理用户疑问、意见、建议、投诉和举报。这也是法律和部门规章所明确要求的。如《电信和互联网用户个人信息保护规定》第 12 条规定的网络运营者应当建立用户投诉处理机制,公布有效的联系方式,并自接到投诉之日起十五日内答复投诉人。这一措施便于进一步明确企业内部责任,防止用户个人信息出现泄露、篡改等问题时无法找到责任人;同时也有利于企业内部更加规范地管理用户个人信息。

其二,建立健全司法救济渠道。用户的权利若得不到有效的救济,法律对个人信息的保护就无法真正的实现。一般而言,公民权利的法律救济包括民事救济、刑事救济和行政救济。

民事救济主要来自民法、侵权责任法等,我国《侵权责任法》《消费者权益保护法》对侵犯个人信息的救济都有相应的规定,被侵权人可以向人民法院提起诉讼。《刑法修正案(九)》将《中华人民共和国刑法修正案(七)》中规定的出售、非法提供公民个人信息罪的犯罪主体由国家机关等单位的工作人员扩大到一般主体,这表明网络运营者若非法出售、提供用户个人信息,情节严重的可构成犯罪。在行政救济上,我国有工信部、各省(自治区、直辖市)通信管理局、工商行政管理部门承担网络用户个人信息保护工作。比如,工信部委托中国互联网协会设立的 12321 网络不良与垃圾信息举报受理中心,该中心不仅受理不良与垃圾信息的举报,同时也处理不良网站涉嫌泄露用户个人信息的举报。对于法律法规未作规定的侵害消费者个人信息的情形,由工商行政管理部门进行处罚。就目前情况来看,受害人在被侵权后的救济渠道多样,多个部门都兼有保护个人信息的职责,因而要整合现有法律制度资源,加强政府管理机构之间的职权分配,由专门机关统一部署,加强各地方个人信息保护行政机构间的执法协作,使网络用户个人信息得到更为有效的保护。

(来稿时间:2018 年 4 月)

参考文献:

1. 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[J].情报理论与实践,2016,39(9):134-139.
2. 应晓敏,窦文华.智能 Web 浏览器及其关键技术[J].计算机科学,2001(9):29-33.
3. 何培育.电子商务环境下个人信息安全危机与法律保护对

策探析[J]. 河北法学, 2014(8):34-41.

4. 刘焕成. 网络隐私保护对策研究[J]. 情报科学, 2003(4):428-433.

5. 宋鹏, 王有凯. 网络背景下个人信息安全保护探讨[J]. 信息网络安全, 2012(8):26-28.

6. 武敏. 云计算环境中的隐私风险和隐私权保护[J]. 出版广角, 2014(10):73-75.

7. 胡水晶. 大数据挖掘的隐私风险及应对策略[J]. 科技管理研究, 2015, 35(9):154-160.

8. 刘小霞, 陈秋月. 大数据时代的网络搜索与个人信息保护[J]. 现代传播(中国传媒大学报), 2014, 36(5):125-128.

9. Smith H J, Milberg S J, Burke S J. Information privacy: measuring individuals' concerns about organizational practices[J]. MIS Quarterly, 1996(2):167-196.

10. 张军, 熊枫. 网络隐私保护技术综述[J]. 计算机应用研究, 2005(7):9-11, 28.

11. 姜明芳. “互联网+”时代用户隐私保护策略研究[J]. 高校图书馆工作, 2017(2):81-84.

12. 曾诚, 庞琳. 大数据时代个人信息安全问题分析[J]. 新闻战线, 2015(4):197-198.

13. 段绩伟. 关于我国信息网络隐私权保护的理性思考[J]. 现代情报, 2007(12):84-85.

14. 梁志文. 论个人数据保护之法律原则[J]. 电子知识产权, 2005(3):10-17.

15. 赵龙文, 郭静. Web 挖掘中公民隐私权保护解决方案探讨[J]. 科技管理研究, 2012, 32(4):151-155.

16. 李雨明, 聂圣歌, 西楠. 大数据隐私侵权界定及其应对策略研究[J]. 图书馆工作与研究, 2017(S):5-10.

17. 李延舜. 大数据时代信息隐私的保护问题研究[J]. 河南社会科学, 2017, 25(4):67-73, 124.

18. 华海英, 孟晓明. 试论基于第三方的网络隐私认证信息服务[J]. 图书情报工作, 2009, 53(6):130-133.

19. 董燕影, 周庆山. 网络隐私第三方认证机制初探[J]. 情报理论与实践, 2009, 32(5):20-23.

20. 徐敬宏. 我国网络隐私权的行业自律保护: 现状、问题与对策[J]. 图书与情报, 2009(5):80-83.

21. Irene Pollach. Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions[J]. Journal of Organizational and End User Computing, 2006(1):23-49.

22. 林旭霞. 论网络运营商与用户之间协议的法律规制[J]. 法律科学(西北政法大学学报), 2012, 30(5):138-145.

23. 谈咏梅, 钱小平. 我国网站隐私保护政策完善之建议[J]. 现代情报, 2006(1):215-217.

24. 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[J]. 当代传播, 2008(6):67-70.

25. 魏来, 郑跃. 隐私 2.0: Web 2.0 时代的用户隐私保护研究[J]. 图书与情报, 2010(5):60-64, 80.

26. 王洪伟, 周曼, 何绍义. 影响个人在线提供隐私信息意愿的实证研究[J]. 系统工程理论与实践, 2012(10):2186-2197.

27. 范慧茜, 曾真. 搜索引擎企业隐私政策声明研究——以百度与谷歌为例[J]. 重庆邮电大学学报(社会科学版), 2016(4):55-60.

28. 陈星. 大数据时代软件产品个人信息安全认证机制构建[J]. 重庆邮电大学学报(社会科学版), 2016(2):39-45.

29. 马民虎. 信息安全法律体系: 灵魂与重心[J]. 信息网络安全, 2007(1):13-15.

A Study on Problems and Countermeasures of Web Browser User Privacy Security Policy

He Peiyu^{1,2} Ma Yaxin¹ Tu Meng¹

(1. Intellectual Property School, Chongqing University of Technology; 2. Postdoctoral Institute, Southwest University of Political Science & Law)

[Abstract] In order to regulate the collection and use of personal information of network users, web browser providers should follow the principles of openness and transparency and formulate sound privacy policies to effectively protect the right to know and privacy of web users. Based on empirical research, the privacy policies of the seven major Web browsers are compared from the general aspects, the terms of information collection and storage, the terms of information usage and sharing. The study found that each Web browser's privacy policy has some problems in terms of the level of privacy protection, the content of the main clauses, and the relationship between rights and obligations. Therefore, it is necessary to start with the formulation and the supervision of the terms of the privacy policy to find a solution path.

[Keywords] Web browser Privacy policy Privacy and security Personal information

[作者简介] 何培育(1983—),男,博士后,重庆理工大学重庆知识产权学院副教授,研究方向:信息法、电子商务法;马雅鑫(1996—),女,重庆理工大学重庆知识产权学院硕士研究生,研究方向:电子商务与网络知识产权;涂萌(1988—),女,法学博士,重庆理工大学重庆知识产权学院副教授,研究方向:知识产权法、信息法。