《厦门大学法律评论》第3期
厦门大学出版社2002.6版
《网络隐私权保护研究》
第101页～第122页

网络隐私权保护研究

周江洪*

目 次

一、引言

网络上所发生的有关信息泄露的问题层出不穷，以至于许多人惊呼："网络让你无处可逃！"例如：1999年1月Intel公司在其P Ⅲ处理器芯片上加上可识别的序列号，触发了隐私权的争论。识别号码的做法可使计算机用户的私人信息受到不适当的跟踪。投诉说，所谓的处理器序列号(PSN)实属不公正和欺骗性贸易行为。包括中国在内的许多国家的政府发出公告要求政府部门抵制含有可识别的序列号的芯片，直到2月份Intel公司宣布可提供相应软件打开或关闭此项功能才使此事告一段落。

cookies工具让你无处可逃：一些网络公司在网页上埋设了具有跟踪功

* 周江洪：厦门大学法律系教师。

能的 cookies 工具测定并跟踪用户在网站上所进行的操作。由于 cookies 具有重塑网络使用者所从事的网络活动的功能，通过对消费者在网络上访问网站、察看产品广告、购买产品等行为的跟踪，结合网络注册系统，就可以得出消费者的健康状况、休闲嗜好、政治倾向、宗教信仰等资料，从而生成有关顾客的个人档案。采用这种方式，美国两家拥有最大规模个人资料库的公司，即 DOUBLE CLICK 和 ENGAGE TECHNOLOGIES，前者号称已掌握了1亿个用户的上网习惯，后者也宣称建立了5200万个用户的个人资料库。①

微软公司 Windows 产品主管 Rob Bennet 在被人揭穿后只好证实，微软的应用软件，如 Word 和 Excel，会生成包含用户个人计算机信息的惟一的确认号码，然后在 Windows 注册过程中被发送出去，微软公司可以根据得到的编码来获取用户的姓名、地址等个人信息。

……

诸如此类的新闻已经不再是新闻，人们对于网络条件下个人信息的安全性越来越担忧。根据 TRUSTe② 2000 年的调查，在美国，隐私权保护或网络安全已经成为电子商务发展最大的挑战，68% 的受调查对象认为只有在隐私权保护得到有效保证的前提下才会从事网络交易；在没有从事网络交易的互联网使用者中，63% 的人最担心的是个人信息的安全；而在网络消费者中，41% 的人最关心的是个人信息的使用情况。③那么，中国的情况又是如何呢？据统计，在网上浏览者中，有45%的潜在消费者由于担心个人隐私得不到有效的保障而放弃了网上购物。④

---

① 郭卫华等：《网络中的法律问题及其对策》，法律出版社 2001 年 1 月版，第 182 页。

② TRUSTe 是目前互联网世界最为著名的网络信息隐私权保护认证机构。到目前为止，已拥有成员 800 多个，与 IT 界领袖 IBM、微软、美国在线、NETSCAPE 等开展隐私权保护领域的合作。

③ Gerhard Steinke, *Data Privacy Approaches from US and EU Perspectives*, Telematics and Informatics, 2002(19), p.194.

④ 梅绍祖等：《电子商务法律规范》，清华大学出版社 2000 年 9 月版，第 84 页。

另外,从隐私权的发展来看,隐私权在其产生之初乃是为了强调国家和个人之间的关系,着眼点在于如何保护个人固有的私密领域不受公权力的侵犯。但是,随着社会的发展,隐私权从国家与个人之间的关系,逐渐发展成个体与他人之间的关系,也就是说,已经发展成个体自我与他人之间的关系,也可以简称为人我关系或者他我关系。在网络条件下,因为由于网络技术的利用使得获取个人信息变得如此简单和便捷,以前需要动用政府才能收集的个人信息现在商家和个人也可以轻而易举地获得,这一他我关系也就表现得更为明显,有关隐私的保护问题变得更为迫切和严峻。

可以看出,隐私权的保护问题已成为困扰电子商务发展的重要障碍。因此,在有关网络规则的研究中,网络信息隐私权一直是学者们关注的主要领域之一。

二、隐私、网络隐私、网络隐私权及相关行为

(一)隐私的概念和内涵

各国对于隐私的定义,由于其法律文化背景的不同而有所不同。美国是目前世界上有关隐私权保护制度较为完善的国家。美国《隐私权法》对隐私进行了这样的描述:"隐私就是指个人希望某些信息不被泄露,信息的范围包括事实,图像(例如照片、录像等),以及毁谤的观点。如果该个人具有适当的敏感,一旦在私人场所透露出的关于他的机密性个人信息被泄露给第三者,可能会使他感到窘迫或情绪压抑。"

我国没有隐私的法律定义,一般而言,法学界将隐私定义为:隐私是指"私人生活安宁不受他人非法干扰,私人信息保密不受他人非法搜集、刺探和公开等"。⑤

这是传统的隐私和隐私权的定义。这一定义是否适合网络条件下的隐私呢?网络条件下的隐私有什么自身的特点?

在网络条件下,与隐私相对应的一个概念是"个人资料"。个人资料确切的包括哪些内容,存在着不同的理解。中国互联网信息中心(CNNIC)对

---

⑤ 张新宝:《隐私权的法律保护》,群众出版社 1997 年版,第 16~17 页。

个人资料内容的表述为:包括用户的姓名、身份证号码、通讯地址、联系电话、电子邮件地址等。许多网站所搜集的个人资料还包括用户的别名或网上的代号,更详细的还有性别、年龄、住址、出生日期,甚至是工作单位等。这些资料主要用于个人的识别,就是自己区别于他人的一种标志。另外,个人资料除了包括个人识别资料外,还包括一些用户的背景资料,一般包括个人职业、受教育情况、收入状况、婚姻家庭状况、工作单位规模、宗教信仰等个人其他信息资料。除此之外,用户在上网的时候,网站设置的计数器会在服务器上自动产生一些其他记录,比如上网的时间、使用的时间、浏览及点击的次数。(如可以统计你上网时所使用的IP地址,你使用的操作系统,浏览器性质等等信息。)另外,利用cookies或序列号等跟踪工具,还可以得到你计算机的有关信息,甚至是计算机上储存的个人资料。

(二)网络隐私权及其分析

隐私权是指"自然人享有的私人生活安宁与私人信息依法受到保护,不被他人非法侵犯、知悉、搜集、利用和公开的一种人格权"。⑥ 或者是指"自然人享有的对其个人的、与公共利益无关、群体利益无关的个人信息、私人活动和私有领域进行支配的具体人格权。"⑦ 按照这些定义,网站所收集的"个人资料"基本上都可以成为隐私权所保护的"个人(私人)信息"的范畴,因为这些个人信息的保护构成了在网络上私人活动或者私人生活安宁的前提。

那么,我们是不是可以说,网络上发生的有关个人信息的保护完全可以采纳传统的隐私权概念及其保护方式呢?

答案是否定的。我们不能无视网络条件下隐私所带来的新的变化。其

⑥ 前引⑤,张新宝书,第21页。

⑦ 杨立新:《侵权法论》(下册),吉林人民出版社2000年3月版,第768页。

中最大的一个变化就是个人数据交易问题⑧ ——在网络世界中，一些公司通过网络技术收集了许多人的个人资料，然后公开出售或者公司之间互换已收集的个人信息。在美国，个人资料的买卖很有市场，而且有逐渐扩展的趋势，例如像 1－800U. S. Search，American DataLink 等大型公司都在从事个人资料的买卖。但是，按照传统的人格权理论，人格利益或者人格权是不能作为财产进行买卖的，这是对人的起码的尊重。按照该信念，个人信息的交易应被完全禁止。但是，从网络经济的本质来说，信息社会里最重要的资源就是信息，因此，为获得竞争中的比较优势，信息的自由流动是完全必要的，如果完全禁止个人信息的交易将妨碍这种网络经济的进一步发展。那么，是否可以说网络条件下，隐私及隐私权发生了质的变化？使得传统的隐私权概念和保护方法不再适合网络需要？

这种看法也是片面的。因为从隐私权的理解来看，一直以来，大都将隐私权仅仅理解成一种具体人格权，而忽视了隐私权所保护的私人信息的属性。按照我们的理解，隐私权得以存在的两个必要前提是：个人信息和个人信息的公开、使用等对个人所形成的私生活安宁的威胁。两部分缺一不可。就前者来说，个人信息本身并没有人格权的属性，而只有在这些个人信息与特定的私生活安宁联系在一起的时候，隐私权才具有了人格权的属性。从这层意义上理解，我们也就可以理解为什么个人信息可以作为一种财产来交易的问题了。也正是从这层意义上来理解，放在网络条件下，我们更愿意将隐私权理解为一种兼具人格权和财产权属性的权利，它当然可以被用来交易，只不过应该利用人格权这一属性限制其交易的方式，交易的目的等

⑧ 或许有人会认为，这并不是网络世界所特有的现象，在真实世界中同样存在。比如电话黄页的问题，从某种程度上来讲也是一种个人数据的出售。但是，我们以为，在真实世界中，个人资料的收集和整理相对比较困难，而且能够从事这种收集和出售的主体相对来说比较少，比较容易监控。而网络技术的运用则使得任何一个个人或公司都可以成为一个个人资料出售者。

等。因此,我们试图这样定义网络隐私权⑨:它是指在网络条件下,自然人享有的对于其个人信息的控制权和处分权,以及与此相关的私人生活不受非法侵扰的权利,是兼具财产权属性和人格权属性的一种权利。

该定义至少包括这几方面的含义,一是对于个人信息的控制权和处分权;前者是指未经网络隐私权人同意,禁止他人非法获取和保留个人信息,后者主要是指权利主体有权按照自己的意志利用(或其他处分方式)其个人信息,未经同意,禁止他人非法利用个人隐私,个人有权控制个人信息的使用和流向。二是积极权能和消极权能的结合——与传统隐私权"免受侵扰"的定义不同的是,该定义揭示了隐私权人对于个人隐私的控制和处分权,以反映网络条件下隐私权保护的特点;三是隐私权同时包含财产属性和人格属性,既属于一种特殊的财产权,也是一种特殊的人格权;从而明确赋予个人信息的可转让性。因为在信息化的网络空间里,商家普遍存在着"信息饥渴症",对于那些涉及消费者的信息有着天然的爱好,消费者信息越来越成为商业竞争的焦点,如果不赋予其财产的属性,很难保证适合这一社会的发展趋势;同时,我们并不把个人信息视为纯粹的财产形式⑩,它始终带有人格的属性,并利用这一属性来限制对于个人信息这一财产的不当使用。从而在赋予个人信息的财产属性的同时,在商家和消费者之间寻找一个合理的平衡点,既能够保护消费者的隐私,保障其获得私人生活的安宁,同时又有利于网络交易的发展。

我们也将以该定义为出发点,展开对网络隐私权的有关分析。

(三)与网络隐私权有关的行为

网络上与隐私权有关的行为很多,但法律问题较多的主要是以下几种

⑨ 该概念的确切表述应该是"网络条件下的隐私权",此处为行文方便,姑且将网络条件下个人对自己的个人信息及其相关的私生活安宁所拥有的权利简化为"网络隐私权"。因此,采用该概念,并不表明本文试图创设"网络隐私权"的概念,只不过将该类现象做一简单的概括,以区别于传统的隐私权,以利于本文的分析和写作。

⑩ 刘静怡提出"信息隐私财产权化"的主张,但我们这里所主张的财产属性是与人格属性相结合的财产属性,而不是纯粹的财产权。详细参考请见刘静怡:《网络社会的信息隐私权保护架构:法律经济分析的初步观察》,刊载于北大法律信息网(http://chinalawinfo.com/research/academy/details.asp?lid=2988),2002年4月18日访问。

行为:个人数据收集、个人数据二次开发利用、个人数据交易以及对个人数据的其他使用方式。

在浏览网页、申请电子邮件或者从事相关的电子商务活动中,我们经常会遇到相关网站要求你输入特定的个人资料,这是一种"明示"的个人数据收集;另外一种情况是你参加网上医疗咨询活动或者其他咨询服务时,咨询者把通过咨询获得的受咨询对象的信息保存在网站中或以其他方式保存。这些都是个人数据的收集。按照传统隐私权和网络隐私权的定义,这种收集本身是否合法,一般而言,没有合法的授权而收集、或者是出于不合理的目的、或者是未经授权非法使用该信息,都将构成对隐私权的侵犯。而完全禁止这种收集不仅不可能,而且也不现实,因为在社会信息化的过程中,一味强求不能保存个人信息无异于放弃计算机文明给人类带来的好处。因此,现在的问题是确定什么人可以收集信息,在什么情况下可以收集的问题。因此,欧洲许多国家都确立了一条原则,"从事信息收集者须在特定的机构进行登记,并且应当说明他们的数据隐私保护政策"⑪。

个人数据二次开发利用是指个人信息收集者把网上收集到的个人数据,存放在专门的数据库中,然后经过数据加工、数据挖掘等方法得到有商业价值的信息或用于其他目的的信息,并用于特定目的的过程。这一过程,从收集者的角度来看,他是通过自己的分析知悉个人隐私的,从目前的实践来看,目的主要是商家为了向顾客提供更多的、持续的服务,以符合消费个性化的潮流。在有关电子商务实践中,一直备受推崇;但从信息被收集者来说,有的人欢迎商家的这种举措,认为是为自己提供了方便;但有些人则感觉个人隐私被泄露,这是对自己私人生活的一种侵扰,最明显的例子就是许多人把个人数据二次开发利用随之而来的广告邮件视为垃圾邮件。因此,如何取舍该问题,仍然需要法律做出相应的安排,以满足不同人的偏好。

个人数据交易则是指在网络世界中,一些公司或个人通过网络技术收集了许多人的个人资料,然后公开出售或者公司之间互换已收集的个人信

---

⑪ Jared Strauss & Kenneth S. Rogerson, *Policies for Online Privacy in the United States and the European Union*, Telematics and Informatics, 2002(19), p.176177.

息。这种交易有可能是单独的个人信息(或数据库)交易,也有可能是连同注册的网站和公司一起拍卖,后者如广州网易。由于其众多的网络用户的信息以相对较高的拍卖价格成交,个人数据交易往往未经所涉及个人的同意,甚至完全在其不知情的情况下进行。因此成为网络隐私权保护的最大威胁。正如前文所指出的那样,网络隐私权是兼具财产和人格双重属性的特殊的权利,完全禁止个人数据信息的交易既不合理,也不现实。因此,如何正视其人格属性,创设一定的规则限制个人数据交易,以保证网络隐私权主体的权利成为电子商务和个人数据交易有序发展的关键。

三、网络隐私权保护模式简介及评价

(一)各种保护模式简评

就网络隐私权的保护而言,目前主要有以下几种建议和实践:

1. 自由放任模式。该模式建立在自由市场模式基础上,是"小政府,大社会"主张在网络隐私权保护领域的诉求。这一模式的支持者认为,网络空间本身就应坚持其自由开放的本质,如果对于网络世界进行过多的干预将使网络的活力窒息。他们相信自由市场这一"看不见的手"将形成最理想的隐私权保护。他们深信,既然经济绩效依赖于通过吸引更多的消费者而不断扩大的市场,商家就会根据消费者的偏好不断调整网络隐私权保护政策。因此,没有外在约束的情况下,自由市场将会自生自发地形成最好的满足消费者需求的网络隐私权保护标准。⑫

但是,自由放任模式所赖以建立的前提——完备市场根本就不存在。只有在充足的市场主体和充分的信息条件下,完备市场及其自由放任模式才得以建立。在信息不对称的网络世界里,如何能够保证商家不断改进规则?如何能够保证网络隐私权的充分保障?另外,由于路径依赖和进出市场机会成本约束的存在,即使消费者可以通过鼠标表现其偏好,但往往不得

⑫ Id. at 179.

不接受商家变更后的不甚合理的隐私权政策声明⑬。

而且,网络隐私权保护的实践也表明,在没有外在压力约束的情况下,光靠消费者的偏好压力本身并不能提供合理的网络隐私权保护政策。⑭

2. 行业自律模式。也就是说,通过行业内部制定行为规章的方式所进行的行业自律。此一主张似乎认为一旦产业界设定了规则,来自于产业界内其它成员的压力,或者来自于市场本身的压力,便可以迫使业界成员持续遵守这些产业内部的行为规章。1998 年美国联邦贸易委员会向国会所做的报告中宣称:"在形成网络隐私权保护政策方面,行业自律是比政府规制更有效、更充分的方法。"⑮该模式的支持者还认为,比起自由放任模式,行业自律采取的是更为积极的姿态,同时认为行业自律模式可以依托行业的专家和信息优势,根据消费者的偏好和商业需要适时地调整其网络隐私权保护政策。

这一模式在美国比较普遍。就目前而言,行业自律的模式主要有网络隐私权保护认证、行业指导规范、网络隐私权保护组织以及安全港等方式。

网络隐私权保护认证计划(online privacy seal program),目前在美国比较有名的 TRUSTE、BBBONLINE 和 SecureAssure,主要都是一些民间机构。也就是说,由这些民间机构对网站或 IT 企业等进行隐私权保护的认证,授予其认证标志,获得该标志的网站可以将其认证标志和认证号码附加在主页等明显的地方,就如同 ISO9000 认证一样。认证机构在消费者和网站等信息收集者之间扮演隐私权保护中介的角色。该方式看起来十分合理和可能,但从实践来看,该方式至少存在以下缺陷:第一,认证的参加者少得

---

⑬ 例如,与此相接近的一个例子是免费电子邮件的问题。但邮箱由免费变更为收费后,邮箱使用人为了避免通知众多联系人的麻烦和对该免费电子邮箱和服务商习惯性的"偏好",往往愿意接受收费信箱,即接受变更后的合同条款。在隐私权保护方面,也可能形成这种路径依赖和机会成本约束问题。

⑭ 虽然从美国电子隐私权信息中心(EPIC)和在线隐私联盟(OPA)的调查可以看出,允诺隐私权保护的网站有日益增长的趋势,但并不能证明是由于自由放任模式的效果所致。See Jared Strauss & Kenneth S. Rogerson, supra note ⑪, at 180.

⑮ Id. at 181.

可怜。TRUSTe和BBBONLINE加在一起,也只有1050个接受认证的网站和其他主体⑯,在所有网站中仅占到可以忽略不计的百分比。大量的信息收集者并没有参加这类认证。第二,认证缺乏有针对性的强制措施,对于违反其认证的主体没有很好的规制手段。以前述的WORD等泄露个人信息的情况,以及MICROSOFT的HOTMAIL存在严重的隐私权保护缺陷为例,作为认证机构的TRUSTe并没有做出很好的反应,甚至没有取消认证。⑰出于自身利益的考虑,认证机构与行业巨头之间暧昧的关系使得其隐私权行业自律保护的可能性正在逐步丧失。第三,认证机构的认证标准存在冲突,阻碍了合理的隐私权保护规则的形成。TRUSTe和BBBONLINE的认证标准就存在着冲突,在没有统一认证标准的前提下,相互矛盾的认证使得消费者十分怀疑认证的公正性和合理性。第四,认证机构独立性的缺乏。认证的目的在于为社会公众提供一个值得信赖的隐私权保护标准,因此,其独立性和专业性将是认证公信力的前提。但是,就如同前述TRUSTe对微软的暧昧态度一样,由于认证主体与接受认证一方的不当利益关联性的存在,在判断是否符合隐私权保护标准时,出于其特定利害关系的考虑,认证主体实际上往往受制于接受认证一方。认证的公信力由于其独立性的缺乏而遭受损害。

行业指导规范模式,就像商会或行会一样,旨在确立行业标准,但其有效性值得怀疑。更何况,行业指导规范本身就可能存在缺陷。根据美国联邦贸易委员会向国会所做的报告,行业指导规范存在许多不合理的地方,并不能有效保证消费者的网络隐私权安全⑱。

网络隐私权保护组织主要是在线隐私联盟(OPA, online privacy alliances)。它向成员提供隐私权保护论坛、促进网络隐私权保护政策的制定,但它只是一个制定政策建议的产业联盟,它本身并不监督成员的遵守情况,也不制裁违反其建议的行为,只是为网络隐私保护提供一些范本。例

⑯ Id. at 183.
⑰ Id. at 183.
⑱ Id. at 183.

如,DoubleClick 和 Real Networks 虽然都是在线隐私联盟的成员,但却一直在从事个人信息交易。因此,其有效性也值得怀疑。

安全港模式是指美国与欧盟之间的一个协议。欧盟主要采取法律规制模式,而不像美国一样倡导行业自律模式。因此,欧盟规定,当成员国的某企业因业务上的需要,要将私人资料传给另一国家的企业或机构时,首先要看这个国家是否有与欧盟大体相同的个人隐私保护措施,否则,欧盟企业不得向其传递有关数据。这一保护模式与美国模式存在明显的不一致的地方,因此无疑在美国与欧洲之间设置了一条贸易和业务交流的障碍。但美国又不可能按照欧盟的要求制定相关的法规,因此,双方最后确立一个"安全港"(safe harbors)机制:凡是那些愿意遵守规定的企业可以签署安全港协议,进入安全港,并获取欧盟企业提供的个人数据;一旦进入安全港,就必须按照欧盟的游戏规则来运作,违规者将受处罚。该模式是国际上对于网络隐私权保护冲突的有意尝试,针对网络的无国界性,对于解决网络隐私权保护冲突具有一定的意义。

总之,从以上有关行业自律模式的介绍和评价也可看出,行业自律模式虽然为网络隐私权的保护提供了一定的可能性,但是,该模式却存在着不可忽视的缺陷。其中最根本的缺陷在于参与主体的缺乏。因为如果我们采取该模式,也就意味着,当我们容忍对个人进行监视的体制,却在这个体制内不赋予受监视的个人应有的参与决策和发言机会时,其实与集权专制体制无异,与网络所倡导的民主和开放背道而驰。隐私权主体没有进入相应的自律组织或参与规则的形成过程,很难保证其权益受到有效的保障。就如同为第三人利益合同一样,在合同的缔结过程中,该第三人完全得看合同当事人的脸色行事,其本身并没有更大的权利。更何况,行业自律模式下的隐私权主体,其地位也还根本没有为第三人利益合同中的第三人所具有的法律地位那样高。

当然,我们也不能否认行业自律模式的意义,毕竟,按照哈耶克的理论,自生自发秩序的形成有赖于行动参与各方的努力。因此,作为隐私权保护中关键的一方主体,其自律本身表明行业规范正在逐渐形成。

3. 自愿或同意模式⑲。该模式也可以称为选择权模式。也就是说赋予个人选择其信息应该如何被使用的权利。目前诸多网络经营者或者厂商所采行的促使个人进行选择的标准方式,则是透过在网页上张贴隐私权保护文本方式做出——也就是借由说明该网站针对隐私权事项所拟定的隐私权政策声明,以及赋予消费者针对该网站处理隐私权的方式选择加入(opt-in)或者选择退出(opt-out)的权利,达成其保护个人信息隐私的目的。

然而,不可否认的是,此种诉诸文本的契约模式,如果要认真执行,处理成本势必相当高昂,然实质意义却相当有限。毕竟,很少有人会有充分的时间或者耐心,去详细完整地阅读那些描述如何控制个人信息流向的模糊规则的繁杂文件,我们甚至不难发现,这种契约模式的可疑之处,很可能在于其基本上已经假设了网络使用者是在完全"自愿"的情况下提供个人资料这一前提,但是,不幸的是,与实际的技术状况对比,网络使用者很可能并不是真正"自愿"提供个人资料的。对于这些格式条款,使用者几乎没有协商修改的可能性,而一旦拒绝提供个人资料给某一特定网站时,结果通常是无法换取进入该网站的权利,在这种片面游戏规则下,网络使用者并无真正选择自由可言。假使未来网络上所出现的主导模式是此种契约规范模式,对于绝大多数的网络使用者而言,提供详细的个人资料很可能成为从事网络活动的"必要之恶",而不是真正获得更多的选择自由。而所谓的"自愿",也很可能是一种"被迫的自愿"而已,因此,这种保护模式应该如何修正,值得进一步检讨与细致化。我们真正需要的,或许是一种能够让某种自动化的代理机制为我们针对隐私权保护问题进行协商的模式,而这个代理机制则熟知使用者在信息隐私权的偏好方面喜欢什么,不喜欢什么。例如,目前麻省理工学院正在开发研制的 P3P 程序,有可能是一个比较好的技术解决途径,后面将对此做一评价。

从上面的分析也可以看出,所谓网络使用者的自主同意,本质上难以完全达成。要使得网络使用者能够在不同的信息隐私保护可能性之间做出完全自主的选择,前提是使用者必须对各个可能性的内涵有充分的理解。然

---

⑲ 前引⑩,刘静怡文。

而,目前的网络现况却绝非如此,毕竟,网络使用者对于其造访浏览的网站,尤其是这些网站搜集个人信息的行为,通常缺乏了解⑳,有时候根本不知道网站正在收集你的个人信息,比如网站在其主页上埋设了"网络侦探"之类的隐蔽技术,使得网络使用者的信息在不知不觉之间被他人获取。因此,网络使用者与网站之间存在着信息不对称(information asymmetries)的现象,而且,对于使用者来说,恐怕也难以细读或理解这些隐私权保护政策的内容。接着,就算隐私权保护政策的内容相当明确,但是面对网络上所呈现出来的标准化隐私权保护契约用语,在种种主客观因素限制下,网络使用者除了同意产业界所共同拟定的格式条款之外,似乎别无选择㉑,换言之,从经济学的角度来看,消费者在面对预设的契约条款时,通常会显现出相当强烈而普遍的惰性,因而放弃进一步的协商,就此而论,我们实在很难推导出网络使用者会有真正自主选择可言。

因此,所谓的同意,从本质上来说,当然必须蕴涵"拒绝"的可能性的存在。但是,由于网络条件下同意模式的缺陷导致了拒绝的实质上的不存在,从而无法利用同意模式很好地保护个人的隐私。

4.技术标准模式。该模式目前也十分流行,支持者主张技术的问题应该由技术本身来解决。该模式中有一种极端的模式是采用完全屏蔽的技术手段,将自己上网所使用的个人计算机的有关信息给屏蔽起来,或者是利用一些黑客工具,可以在不输入个人信息的情况下直接进入网站。后者是黑客技术的滥用,与前面所讲的黑客人侵计算机系统的性质一致,几乎所有的国家都否认这种保护方式。前一种模式由于将个人信息完全屏蔽起来,使得国家在为了公共利益的情况下也无法获得个人的信息。因此,各国经过一段激烈争论后,基本上都否决了这一模式。

因此,我们需要一种机器对机器的技术标准(machine-to-machine proto-

---

⑳ See Neil Weinstock Netanel, Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, 88 *Cal. L. Rev.* 435~40 (2000).

㉑ 有关集体行动的典型 See generally Cass R. Sunstein, *Free Markets and Social Justic*,59~61 (1997).

col),为我们协商隐私权保护事宜。一旦使用者设定了自己的隐私权保护偏好——也就是将使用者个人愿意以何种方式进行隐私权保护协商,以及其愿意放弃哪些保护的选择予以特定化——使用者个人一旦进入某一网站,该网站和使用者所使用的机器本身便开始进行磋商,惟有在使用者的机器和该网站取得协商合意的结果时,该网站才能取得使用者的个人资料。现在讨论比较多的模式是来自美国麻省理工学院的P3P模式。

美国麻省理工学院的万维网联盟(WWW Consortium)所资助的名为P3P(隐私权偏好等级计划平台,即the Platform for Privacy Preference Project)的计划,是一种可以让使用者和信息收集者之间透过类似等级一到五的模式,协商出隐私权保护方式的通讯协议,其目的在于促成一个使用者可以表达其隐私权保护偏好,并且针对其个人信息的使用进行协商的架构[22]。举例来说,如果我对隐私权十分坚持在意的话,那么我或许愿意付出较高的代价,去使用某一家能够保证提供给我等级较高的隐私保护的网站。相对地,另一个人可能一点也不在乎隐私权保护的问题,则可以以较低的代价,选择使用仅提供较低等级的保护。从某个角度来说,这其实就是网际网络的运作现状:网站通常提供我们各种免费信息,而网络使用者则是提供他们的个人信息,当做交换条件,透过这种技术标准作为代理机制的模式,我们可以让协商与交换过程在网络世界里具体普及。

当然,P3P仍然面临各种技术[23]、政策和法律障碍,克服这些问题之后,方有落实机会,但是P3P的出现,却的确引导我们可以在网际网络的科技基础上想像并规划出类似的信息生活架构,这个以科技大幅降低我们在信息生活中所面对的交易成本的架构,应该与某个市场互相结合,以现实世界里的任何机制都无法企及的方式,以随时尊重自主选择的方式保护我们的信息隐私权。

---

[22] See Joseph M. Reagle & Lorrie Faith Cranor, The Platform for Privacy Preferences, *Communications of the ACM*, Feb. 1999, at 48

[23] 例如,P3P必须要求所有的服务器和使用者电脑之间存在着一个类似TCP/IP一样的标准协议,而从目前现状来看,这一标准协议实现的可能性甚微。

但是,该模式从本质上来说,仍然属于同意模式。因此,有关同意模式的缺陷仍然存在。更何况机器或程序的设置虽然降低了交易成本,但却增加了其僵化的性质,在某种程度上而言是放弃了可以充分协商的机会成本,因此,对于其降低的交易成本到底如何仍然值得讨论。而且,该技术本身的安全性问题值得怀疑,随着技术的进步,不排除有可能某些用以收集信息的软件能够绕过该平台而达到收集利用消费者个人资料的目的。而且,该类软件的变通性较小,不能限制网络信息收集者对于信息的进一步利用。消费者的选择权仅仅存在于进入网站的那一刻,内容仅限于是否许可收集,限制性较大。因此,技术保护只能成为一种辅助的手段,不能代替法律的规制。

5. 财产权模式。该模式将网络使用者的个人信息视为财产加以保护,该模式正趋于流行㉔。其实,在 P3P 模式中,也蕴涵了一种财产的观念。按照财产权规则,如果想要拥有财产权的人,必须在取得财产权之前先进行协商和谈判。P3P 正是促成和简化这种谈判协商的技术平台。

在网络时代里,此种财产权模式乃是将个人信息视为可以分配给和该等信息有关的个人予以控制的资源,或者分配给该个人以外的商业经营者控制的使用的资源㉕。将信息隐私权理解为具有财产权性质一般的控制权能。

这一模式至少解决了咱们前面讲述的网站是否有权转让收集的个人信息问题,将个人信息(隐私)视为一种财产,就解决了转让合法性的关键,否则,作为人格权而言,一般是不允许转让的。

该模式的最主要缺陷在于,将隐私及隐私权看成纯粹的财产权,姑且不说人格的异化问题,就实践操作而言,也将引起更深层次的法律难题,犹如"饮鸩止渴"。因为如果按照财产权的规则,当某人取得财产权以后,就可以随意处分自己的财产,因为他个人对自己的财产享有完全的处分权。如果

㉔ 前引⑩,刘静怡文。

㉕ See generally Pamela Samuelson, Privacy as Intellectual Property?, 52 *Stan. L. Rev.* 1125 (2000)

结合隐私权问题,就有可能发生这种问题,当某网站通过购买方式取得用户的个人信息以后,他可以任意处分其个人信息,比如将其倒卖、篡改,从而有可能发生用户的个人信息被某些用户并不希望其看到自己个人信息的人获得,从而损害用户个人的利益。这就是赋予隐私财产权性质容易导致个人对自己的个人信息丧失控制权的问题,从而可能引发严重的社会问题。

6.欧盟的立法规制模式。早在互联网的起步阶段,欧洲人就意识到了保护网络隐私权的法律问题。1998年10月,欧盟在1995年《关于个人资料的运行和自由流动的保护指令》的基础上制定了《电子商务私人资料保护办法》开始生效。它十分严格地限定在传递和使用个人信息数据时必须遵守的规则。公司或网站如果要收集或使用某人的个人信息,应先告知该信息将被做何使用,而且需要其本人的同意。另外,个人不仅有权了解这些资料和数据,只要他愿意,还可以做删除或修改。从立法层面上确立了个人对其私人信息的最终控制权。

(二)小结

以上几种模式实际上可以概括为两种模式,一种是法律规制模式。该模式的特征在于赋予隐私权主体对于个人隐私的积极的控制权,而不是传统的个人隐私"免受侵扰"的消极保护。另外一种是自律模式,该模式的特征在于通过隐私权法律关系当事人之间的自力救济和自我约束来实现对个人隐私的消极的保护。可以这么说,前者是国家的积极介入,而后者是倡导自由的市场模式的反映。而不同的文化背景和社会发展状况导致了美国与欧盟保护模式的不同选择。安全港计划则试图在两者之间达到国际范围内的妥协和结合。

五、关于我国网络隐私权保护的建议

(一)我国网络隐私权保护现状

我国在公民隐私权的保护方面,除了将其纳入名誉权保护范围之外,尚无更加明确的法律规定,这一保护方式的缺陷学者多有论述,此处不加讨论。而在网络隐私权方面,并无专门法律来保护网络中的个人资料安全。到目前为止,只有2000年11月7日信息产业部发布的《互联网电子公告服

务管理规定》中规定,“电子公告服务提供者应当对上网用户的个人信息保密,未经上网用户同意,不得向他人泄露”,违反该规定的,由电信管理部门责令改正,给上网用户造成损害或者损失的,应依法承担法律责任。这一规定只规定了 BBS 中有关个人隐私的保护问题,而没有涉及到其他网络活动中的个人隐私的保护问题,已不能满足人们对隐私权保护的需要,在网络迅速发展的条件下更需尽快改进。

(二)我国网络隐私权保护的原则建议

基于前述网络隐私权保护模式的分析及中国网络隐私权保护的现状,我们认为在未来的网络隐私权保护制度选择上至少应考虑以下原则:

1.信息的自由流动与对个人信息的保护并重原则。网络社会本质是一种通过信息联结起来的人类活动方式,因此,信息的自由流动乃是网络生命力所在。但是,对人的权利的保护“只有当它包括了获得安宁的权利时才能对一个人的尊严提供全方位的保护”,而“所有将人格权从宪法的角度列为基本人权的国家也都在民法的层面上理所当然地规定:‘必须尊重他人私生活中的隐私’。”㉖ 对隐私及隐私权的保护就构成了“人之所以为人”的重要前提。所以,必须在两者之间寻找一恰当的平衡点。也正如同前面所言,网络隐私权具有人格和财产双重属性。该原则正是基于以上考虑,试图在财产与人格之间寻找一平衡点,以保证促进社会信息化的同时而不导致人自身的“异化”,无论如何,免受侵扰的个人空间永远是人得以自由自在的前提。

2.个人信息使用的最小化原则。一个人的个人信息越是公开化,他就越是处在被他人“观看”(“监视”或“控制”?)的位置上。这就好像一个演员处于舞台灯光的直接照耀下一览无遗,而处在灯光照射之外的观众则在安全地带一样。个人自由空间的缩小,意味着他始终处在一种无形但却是强大的公众压力之中。因此为了缓解这一来自网络世界的压力,对于个人信息的公开收集或使用必须被限制在最小的范围内,以保证个人私生活的安

㉖ [德]克雷斯蒂安·冯·巴尔:《欧洲比较侵权行为法》(下卷),焦美华译,法律出版社 2001 年版,第 131 页、第 135 页。

宁和自由。

3.明确界定信息收集者和信息被收集者之间的权利义务关系原则。

从目前行业自律模式和法律规制模式的实践中可以归纳出,一般来说,一项合理的网络信息隐私权保护政策至少需要满足以下几个要素,我们界定权利义务关系也可以从这几方面出发:

(1)告知义务(notice)。该要素若从信息被收集者角度看,也可以表述成知悉权。在传统的法律实践中,信息被收集者一般都拥有知悉权。例如,日本1990年实施的《关于保护行政机构与电子计算机处理有关的个人信息法律》第13条明确规定,任何人都有请求阅览行政机关保存的个人信息的权利。而在网络隐私权领域,该要素可以做如下表述:信息收集者应当明确告知信息被收集者收集的信息范围、信息的收集方法以及这些信息将被如何使用、将与谁一起分享该信息和信息的流向等。这里必须强调的是利用特殊软件收集个人信息的情况,信息收集者必须告知他所利用的软件及其运作的一般过程或原理,如cookies工具。信息收集者对于这些埋设在服务器内的工具很难知晓,因此也就无从知道信息的被收集过程。因此,告知义务乃是合理的网络隐私权保障的前提条件。这也可以看做是消费者知情权的表现之一。

(2)选择权(choice)。该选择权即前述的同意模式,其本质在于赋予个人选择其信息能否被收集以及应该如何被使用的权利。这也是法的一般原理的体现:任何人都不得在未经本人同意而违背其意志的情况下被亮相于公众;非公众人物有获得安宁的权利;而公众人物也有避开公众眼光独处的权利。[27] 但是,这种选择只是选择能否收集,而没有对隐私权主体其他相关权利充分关注,难免保护不全,因此我们这里所说的选择权是指应当赋予信息被收集者控制其个人信息的被收集和利用的绝对权利,不仅包括是否允许被收集的选择,还包括选择如何被使用的权利。特别应该说明的是,该选择本身不应该具有不可变更的效力,信息被收集者有权单方面变更其选择,也就说,如果没有特别约定或说明,信息被收集者可以单方面解除信息的使

---

[27] 前引[25],克雷斯蒂安·冯·巴尔书,第124页。

用合同。否则,当事人将不得不受制于那些由于自己一时的不慎而确立的个人信息使用合同,难免不公。

(3)访问权(access)。该项权利的赋予主要在于保证个人信息被正确合适的收集,与知悉权相辅相成。要求信息收集者允许信息被收集者方便地访问或查阅自己的信息,并赋予信息被收集者更正不正确的个人信息的权利。早在1976年的德国《联邦个人资料保护法》中就规定个人有权查阅和更正有关本人的资料,在资料不正确或不完整的时候,还有权阻止资料的储存。[⑧] 这也可以表述为一种要求信息与其背后的"身份上一致性的权利"。否则,错误的信息将导致个人信息所表征的主体的错误的人格形象。

(4)安全(security)。该要素要求信息收集者保证个人信息在储存、传递和使用过程中的安全。也就说,信息提供者应尽可能地阻止信息的泄露、丢失、毁坏、篡改或没有授权的接触。

(5)联系的可能性(contact)。该要素要求信息收集者应当提供方便的联系途径,以保证信息被收集者能够及时方便地与信息收集者联系。这是信息被收集者能够行使上述诸项权利的前提条件。

以上五个要素逐渐成为网络隐私权保障的标准条款,逐渐成为行业自律模式和法律规制模式共同倡导的网络隐私权保障的一般要求。[⑨]

4.对网络隐私权的保护实行法律规制和行业自律并重原则。如前所述,行业自律虽有其合理性一面,但由于其内在的缺陷,规则形成参与主体的单方性所导致的规则的单方性,使其不可能有效保护网络隐私权;而法律的规制则会由于其固有的僵化和保守性格,也难以完全处理网络隐私权问题。因此,建议采纳该原则。这也是规则形成的一般规律的反映:规则的形成在于内生秩序和外生秩序的共同促进。而且,实践也表明,目前的网络隐私权保护也正走向这一目标。除了前述安全港建议之外,美国联邦贸易委员会和国会以及其他机构正在努力采取立法规制模式克服其行业自律模式

---

⑧ 前引①,郭卫华书,第177页。

⑨ Jared Strauss & Kenneth S. Rogerson, *Policies for Online Privacy in the United States and the European Union*, Telematics and Informatics, 2002(19), p178.

之不足。2000年5月22日,联邦贸易委员会通过了本年度关于消费者在线隐私的国会陈词——"在线隐私:电子市场中的合理信息实践(online privacy: the fair information practice in the electronic market)"。联邦贸易委员会认为尽管行业自律的努力取得了许多实质的进展,但是这种通过行业自律保护消费者在线隐私的制度缺乏执行机制,为了充分保护消费者的个人信息以及树立公众对于电子商务的信心,需要国会就此制定法律。建议国会立法以保障网上消费者最低的保护水平,并建立网上收集个人信息行为的起码标准。就我国而言,当欧盟和美国都倾向于立法保护网络隐私的时候,显然是在促成全球范围对于消费者在线隐私政策的趋同,都试图用立法来规制个人信息的收集和使用问题,这对于我国未来的电子商务发展而言,也会带来一定的立法压力。就如同中美知识产权谈判给我们所带来的压力一样。

5.坚持网络隐私权保护人格属性和财产属性并重的原则。可以这么说,前面四个原则在一定程度上都是立基于该原则,都是在确保个人对于其个人信息拥有的控制权和处分权的前提条件下形成。

6.保障信息被收集者参与规则制定的原则。该原则主要是针对行业自律模式所存在的不民主方式所做的努力,试图通过主体的参与引导新的行业自律模式。

7.采取必要的技术手段原则。这也是对于前述技术保护模式合理性一面的承认。在网络世界中,技术手段也将是促进人自身的解放和人自身自由实现的重要手段。另外,技术的手段也需要法律加以规制。但法律对技术做出规制的时候,尚需注意"技术中立"的原则[30],也就是说,对于各种保护网络隐私的技术,应注意既不能厚此薄彼,也不能妨碍技术的进步。

(三)我国网络隐私权保护的规则建议

立足于上述原则,结合前述各国网络隐私权保护模式的评价,我们以为将来的网络隐私权立法至少应该包含以下内容:

---

[30] 关于"技术中立"的详细讨论,可参见张楚:《电子商务法初论》,中国政法大学出版社2000年版。

1. 承认个人信息的可转让性。前述论述可以看出，网络隐私权较传统隐私权而言，其保护重心已逐渐地由“独自享有”、“不愿公开”、“免受侵扰”等消极方面，而转移为“个人信息资料的利用与控制”的积极方面来了，因此，承认个人信息的可转让性乃是网络隐私权保护的首要所在。个人信息的转让，其实质是个人信息利用权的转让，但是，由于网络隐私权的人格属性，可以规定采取许可合同方式进行转让，指定许可合同的各种规则。如许可合同的种类、许可合同的限制等等。一般来说，没有特别约定，个人对其本人的个人信息拥有最后处分权。

2. 建立强制性的网络隐私权保护登记制度，鼓励开展隐私权保护认证制度。法律应该规定，信息收集者在从事相关的个人信息收集以前，必须到有关部门登记，在没有取得登记以前，不得从事相关的信息收集行为。违反登记义务，应追究相应的责任。同时，鼓励开展隐私认证制度，这是吸收行业自律模式的必然反映。可以参照质量认证体系做出相应的认证规范。同时，对从事网络隐私权认证的机构进行严格的资格审查和年检制度。这是保证网络隐私权认证机构独立性和公正性的重要条件。

3. 在网络隐私权保护的救济中，赋予受害人救济方式和责任方式的选择权。当事人可要求侵害人承担侵权责任，也可以根据个人信息许可使用合同要求承担合同责任。在举证责任方面，可以要求占有信息和技术优势的网站或经营者承担举证责任。

4. 在保障网络隐私权主体的权利的同时，也应当确保个人信息收集者的合法权利。个人信息收集者对于其合法取得的个人信息和经授权使用的个人信息在法律范围内享有充分的占有和使用权，非法侵犯其权利，也可以要求行为人承担相应的责任。这是促进信息社会发展的必然。

5. 赋予信息被收集者的参与制定规则的权利。“只有公正的程序，才具有产生公正结果的能力”[31]。规则的形成亦是如此。可以考虑采用类似价格听证的制度，要求规则（包括行业自律规则）的形成必须要有作为信息被收集者的消费者代表参与，并制定相关的具体规则，以保证网络隐私权保

---

[31] 沈宗灵主编：《法理学》，高等教育出版社 1994 年版，第 49 页。

护规则形成的民主化和合理化。

总之,针对网络隐私权这一新的权利形式,应当在实现对个人权利和家庭价值的尊重的前提下,通过行业自律、法律规制和当事人的共同努力建立合理规则体系。网络社会的发展也将由于这一合作的范例而在协商中不断进步。