北京商报 BEIJING BUSINESS TODAY
新|闻|启|迪|财|智

IT 互联网周刊
IT&Internet Weekly

总第145期 今日4版 每周三出版
新闻热线 8610-84285566-3153
主编 罗添

C1–C4
2013.3.27

C2 智能拨号软件打防骚扰牌

Cookie危机和App窥私风险在挑战行业神经，公众最易遇到的骚扰电话和骚扰短信，传统的安全软件通常束手无策，而移动互联网创新公司正在致力于解决此现象，还用户一个绿色的通讯环境。

C3 团购传统淡季首次回暖

历经四个年头的团购行业首次淡季实现逆转。根据团购导航网站团800数据显示，今年前两个月团购总成交额破43.3亿元，环比增长7.4%。而在过去，每年一二月是团购淡季，销售额均会低于前一年年底业绩。

C4 视频再不进军移动和大屏就晚了

“网络视频未来的变革趋势是移动与大屏一个都不能少”，聚力传媒副总裁单晓蕾十分肯定地说，为了抢先占据电视端用户，他向北京商报记者透露，PPTV将在下个月推出新一代智能互联网机顶盒产品。

是工具还是黑手

央视“3·15”晚会让一个互联网专业技术名词一夜间走进了公众的视野，它就是Cookie，中文的意思“小甜饼”。由于它记录着用户上网的行为以及上网特点，可以让网民快速使用互联网服务，而无需每一次都要重新输入信息，一方面为网民带来了上网的便利，而另一方面却埋下了安全隐患。一些网络公司通过收集用户的Cookie信息来分析用户的上网行为，进而贩卖给广告商。

对于广大网民来说，Cookie到底是工具还是黑手一时间成为业界争论的焦点。为此由北京商报主办的“科技青商汇”论坛特邀请技术、行业、媒体、法律四方面人士解读Cookie引发的隐私安全风暴。

Cookie无罪：别指摘

“Cookie就像菜刀，是厨房好帮手，但有人却拿来行凶，说到底菜刀本身是无罪的”，知名知识产权律师、北京德和衡律师事务所合伙人姚克枫如是定义被视为“洪水猛兽”的Cookie。

一般来讲，Cookie就是用户数据包，它记录着用户上网的行为、上网特点以及上网输入的文字，甚至是用户名、密码，也可能包含其他隐私内容。因为央视“3·15”晚会的曝光，个别互联网公司滥用Cookie，这一词汇甚至成了与网络风险画等号的“洪水猛兽”。

但北京邮电大学信息安全中心副教授辛阳认为，Cookie是无罪的。他进一步解释称，“企业采用Cookie的初衷是为了让用户更便利地使用服务，而不必每次上网都重新载入个人信息”。

对普通网民来说，Cookie主要用来判定注册用户是否已经登录网站，这样可以免去用户重复登录网站的繁琐，试想如果用户每刷新一次微博、邮箱都需要重新登录，将极大影响用户体验，想必就没有多少人愿意再上网交流了。Cookie的另外用途是网上购物的“购物车”功能：网民可能会在一段时间内在同一家网站的不同页面中选择不同的商品，这些信息都会写入Cookie以方便最后网购结账。

事实上，在Cookie引发争议之后，行业也在探索解决之道，有的建议“禁掉Cookie”。博客中国副总裁谷龙介绍，谷歌最新的浏览器已经提供关闭Cookie的功能，但负面效果是上网变得非常慢，需要反复确认用户身份，带来了种种不便。

“Cookie禁了也没用，”辛阳说：“有心使坏的企业还会找到其他方法读取用户隐私，比如App软件的服务器端就可以进行读取。”

企业有责：别滥用

目前Cookie引起强烈争议的就是互联网企业通过分析Cookie研究用户上网行为，再精准广告定位而引发的隐私泄露问题。

很多人不了解Cookie在隐私泄露中扮演的角色，实际上是不法企业利用Cookie存储用户信息的特性，使用一种叫做“网络臭虫”的方法来获取用户Cookie，分析上网行为。

譬如，在一些访问量巨大的网站植入一段臭虫代码，这样“网络臭虫”就可以收集访问该网站网民的Cookie数据。由于Cookie数据中包含着诸如网页浏览器、停留时间、购物商品等个人偏好信息，因此个人信息被“网络臭虫”截取，这些企业统计分析这些个人信息后，卖给其他互联网公司牟取暴利。如果一个被植入“网络臭虫”的网站一天一个页面有1000万人访问，那么这个试图窃取的公司一天就获取了1000万份个人信息。收集Cookie这种行为在互联网领域并不罕见。譬如搜索引擎服务提供商及其联盟网站，每天大约跟踪1.2亿网民的Cookie。如果这些Cookie被泄露，将会让互联网基本信任体系崩盘。

为此，创新工场CEO李开复建议所有网站，首先要告知用户哪些信息被使用，其次保证不滥用信息，最后提供“禁止跟踪”选项保护用户隐私。诸如微软、谷歌，国内的360、搜狗均已采取类似行动。

资深媒体人、《商业价值》主编张鹏表示，企业在收集用户个人信息时要特别慎重“用户的个人信息相当于个人财产，上传个人信息的目的是换取互联网服务，这必须是透明和等价的交换”。

不道德的企业借机搜集用户数据，借口是必须使用用户位置或通讯录才能完成某项服务。辛阳担忧，普通公众很难判断一款互联网服务索取哪些个人信息是合理的。

法律呼声：必先行

其实，不仅仅在国内，网络个人隐私信息的安全也是全球化的议题，包括微软、谷歌、苹果等巨头在内的众多互联网公司都已经全面推出清除“跟踪Cookie”的行动。

“企业自律，也应该有行业自律，把Cookie使用规则、隐私问题上升到行业规范，把基本标准制定出来，可能是比较好的监督机制。”姚克枫坦言，国内对隐私保护的法律法规尚不健全，而具体到Cookie这样细化的法规也不太现实，行业可以先行制定行规。

“解决隐私问题要相信市场，相信竞争，谁做了坏事，用户自然会用脚投票。行业要自律，把事情说清楚和讲到位，让市场充分选择。”张鹏如是认为。

姚克枫建议，行业自律应该涉及“个人信息什么情况下使用是妥当的，什么情况下使用是不妥当的”，“企业如何利用Cookie，不给第三方网站泄露内容”也应该列入自律之列。

另一种必不可少的方法是第三方安全认证机制和机构。企业自说自话无法让舆论信服。然而企业自律和行业自律永远是预防为主，在隐私泄露不可能完全杜绝的今天，法律层面的惩戒意义才是长远之计。据悉，国外已经有很健全的法律准则和环境去推进互联网隐私保护。去年，美国联邦贸易委员会就对谷歌做出罚款2250万美元的决定，原因是谷歌涉嫌通过浏览器追踪用户。而在国内，之前发生的天涯论坛泄露4000万用户数据等事件中，当事企业并未受到来自监管部门的实质性处罚。

“我希望法律更健全一些。至少对隐私、互联网隐私、隐私泄露有更明确的法律定义，这样有利于行业由此制定自律规则，也能在严重事件后保护用户知情权、同意权”，姚克枫坦言，每年国内因互联网隐私泄露宣判的案件还很少。

观点

Cookie泄露隐私 是安全厂商集体失职

在“3·15”晚会曝光互联网公司通过Cookie泄露隐私是行业潜规则的同时，安全厂商也该集体反思自己的失职。

实际上，Cookie中保存的用户名、密码等个人敏感信息通常经过加密，很难将其反向破解。但这并不意味着绝对安全，黑客可通过木马病毒盗取用户浏览器Cookie，直接通过偷取的Cookie骗取网站信任。可以看出，木马病毒入侵用户电脑是导致用户个人信息泄露的一大元凶。

自1993年Cookie诞生以来，其就拥有专属性原则，即A网站存放在Cookie中的用户信息，B网站是没有权限直接获取的。但是，现在一些第三方广告联盟的代码使用范围很广。这就造成用户在A网站搜索了一个关键字，用户继续访问B网站，由于B网站也使用了同一家的第三方广告代码，这个代码可以从Cookie中获取用户在A网站的搜索行为，进而展示更精准的推广广告。比如搜索“糖尿病”等关键词，再访问其联盟网站，页面会立刻出现糖尿病治疗广告。如果并未事先告之，经用户同意，此做法有对隐私构成侵犯的嫌疑。目前这个还处在灰色地带。

因此，跨站Cookie恰恰就是用户隐私泄露的罪魁祸首，所以限制网站使用跨站Cookie，给用户提供禁止跟踪(DNT)功能选项已成为当务之急。据了解，目前IE、Chrome、360、搜狗等浏览器均可以快速清除用户浏览器网页的Cookie信息。但从目前整体的隐私安全保护环境来看，安全软件仍然存在着巨大的防护缺口。所以安全软件也可以并且有必要提供定期清理网站Cookie，并监测跨站Cookie使用的功能，保护用户隐私安全。

北京商报记者 张绪旺/文 张淼/漫画

主管副总编辑 雷雅梅 编辑 罗添 美编 张淼 责校 池红云 E-mail：shangbaoit@163.com