● 王树义，朱　娜（天津师范大学　管理学院，天津　300387）

移动社交媒体用户隐私保护对策研究*

摘　要： 移动互联网的社交、本地及移动属性为社交媒体带来了新的特点，这一新环境对社交媒体用户隐私保护提出了新的挑战。文章分析了移动互联网环境下社交媒体用户隐私泄露的方式、原因，并有针对性地提出了移动互联社交媒体用户隐私保护的对策与方法。

关键词： 移动互联网；社交媒体；隐私保护

Abstract: The social, local and mobile attributes of the mobile Internet have brought new characteristics to social media, and this new environment presents new challenges to social media user privacy protection. This paper analyzes the types and causes of the disclosure of social media user privacy in the mobile Internet environment, and proposes some pertinent countermeasures and methods for the protection of social media user privacy on the mobile Internet.

Keywords: mobile Internet; social media; privacy protection

随着移动通信技术的进步，移动宽带飞速发展。高性能的智能移动终端逐渐普及，移动互联网正逐步改变人们的生活方式。有“互联网女皇”之称的玛丽·米克尔发布的《2012 年互联网趋势报告》显示，截至 2011 年底，全球互联网用户接近 23 亿，同比增长 8%。全球移动 3G 用户为 11 亿，同比增长 37%[1]。

据中国互联网信息中心发布的《第 30 次中国互联网络发展状况调查统计报告》显示，截至 2012 年 6 月底，中国的网民数量达到 5.38 亿，增长速度平稳，其中手机网民规模达到 3.88 亿，手机首次超越台式电脑，成为第一大上网终端[2]。

与此同时，社交网站也开始了向移动互联网转移的大趋势。伴随着用户方便与快捷的新体验，用户安全与隐私保护遭遇的问题也日渐突出。2012 年 10 月，信息安全领域全球领先的提供商赛门铁克对来自 24 个国家或地区的 13 000 多位成年人进行了调查，研究报告揭示出新型网络犯罪正转向社交网络或移动设备网络。仅 2011 年，网络犯罪便致使全球个人用户蒙受了高达 1 100 亿美元的直接损失；而在中国，估计有超过 2.57 亿人成为网络犯罪受害者，43% 的网络成人用户遭受过社交网络或手机网络犯罪的侵害[3]。社交媒体用户的隐私是网络犯罪罪犯的重要目标。

与上述现象形成鲜明对比的是，越来越多的人不介意在社交媒体上提供自己各方面的信息，而是热衷于在社交网站上展示和分享自己的生活。据《第 30 次中国互联网络发展状况调查统计报告》显示，在社交媒体隐私设置上，23.5% 的用户将信息设置为所有人都能看到，13.4% 的人表示不清楚自己的设置，也就意味着没有关注过这些安全问题，这证明相当一部分的网络用户没有注意到隐私保护的重要性[2]。

本文针对目前移动社交媒体用户隐私泄露的原因并提出针对性的对策建议，具体来说，本研究旨在回答以下两个具体问题：① 移动社交媒体用户隐私泄露的方式和原因有哪些。② 保护移动社交媒体用户隐私的有效对策有哪些。

1　移动社交媒体用户隐私研究

2011 年 2 月著名风投、美国 KPCB（Kleiner Perkins Caufield & Byers）风险投资公司合伙人约翰·杜尔（John Doerr）提出了“SoLoMo”这个概念。他把最热门的 3 个关键词整合到了一起：Social（社交化）、Local（本地化）和 Mobile（移动化），以此来概括移动互联网的特点。同时也有研究者分析了在这种背景下移动社交网络（MSNS）较之于传统社交网络（SNS）的新特点。并概括为 4 点：基于活动，移动性和基于情境，依靠移动设备，开放平台[4]。

移动社交网络不仅仅是传统桌面社交网络的无线版本，而是更具动态和交互特性、内容更加丰富的个性化社

* 本文为教育部人文社会科学研究青年基金项目“基于群体智慧的微博客信息可信度评价机制研究”（项目编号：12YJC870025），天津市高等学校人文社会科学研究项目“基于复杂自适应系统视角的微博客信息甄别机制研究”（项目编号：20112148）和天津师范大学博士基金项目（项目编号：52WW1103）的成果之一。

交应用。

关于社交媒体用户隐私保护问题日益受到学术界和工业界的关注。主要研究集中于用户隐私保护范围和认知[5-7]、服务提供商隐私保护设置[8-9]、国家法律行业政策[10]、隐私攻击模式和保护等方面[11-15]。

对于隐私攻击和保护模式，研究者主要从基于网络结构的再识别攻击、推理攻击、信息聚集攻击和传统的属性再认证攻击等方面进行分析。关于结构再识别攻击，研究者主要从匿名处理方面提出保护，且研究较充分。但是随着网络规模的扩大，再识别攻击将变得更加困难。因此保护社会网络上发布的信息本身，对用户而言具有更大的实际意义，而这方面的研究还很有限。

罗波提出对于目标用户，攻击者可以收集他有意无意泄露的各种零碎的个人信息，尽管一小片信息看上去并无价值，但是如果攻击者将这类信息关联起来（即信息聚集），往往会导致严重的后果。对此他提出了隐私监视器的概念，因为监视器可以主动地收集与用户有关的信息，模拟信息聚集攻击并将结果提交给用户，从而使得用户可以实时地监控自己发布在各个社交网站的信息，保护自己的隐私[13]。

E. Zheleva 指出在很多社会网络中，用户可以选择公开或者隐藏自己的私人信息，然而，即使用户自己的信息被隐藏，有些属性仍然可以通过公开的朋友信息而被泄露，即推理攻击。Zheleva 提出社交媒体应当设置保护用户朋友关系或者群组关系的设置并引起用户的注意[15]。上述研究成果对于移动社交媒体用户隐私保护也有很好的指导作用。

对于移动社交媒体用户隐私保护的研究，主要集中在对 LBS 的位置信息保护。其中对于服务提供者获得的用户位置信息的保护技术主要分为两类：基于匿名技术的保护，其主要目的是保护用户身份信息和敏感信息的链接；基于模糊技术的保护，其目的是通过降低精确度来保护敏感信息[16]。

也有研究者从用户需要的角度出发，提出了为用户提供既有利于隐私保护也便于社交的位置分享模式。例如根据用户之间的关系亲疏设置位置信息公开的程度。上述研究虽然对本研究具有一定的借鉴意义，但没有能够将 LBS 与 SNS 相结合，对隐私保护进行探究[17]。

当前大部分研究并没有将移动社交网络看成一个整体，或者只关注了“SoLoMo”中的 Lo（本地化）的部分。本文在借鉴传统社交网络以及 LBS 隐私保护的基础上，结合移动社交网络的新特点，尝试从用户角度出发研究移动社交媒体用户隐私保护问题，以期提出综合化的隐私保护框架。

2 移动社交媒体用户隐私泄露方式和原因

在分析移动社交媒体用户隐私泄露方式之前有必要对隐私类别进行分析，除了传统的用户身份、身体状况、家庭背景、社会关系等之外，出现了一类新的隐私即位置隐私。

2.1 移动社交媒体用户的位置隐私

移动社交媒体并不只是传统社交网络的移动化，因此需要针对其特点进行更加深入、准确的分类和研究。根据 2012 年 9 月苹果 iTunes（中国区）里排列前 30 位的社交应用，可以将移动社交媒体大体分为 3 类：①传统 SNS 类：包括新浪微博、腾讯微博、Facebook、QQ 空间和人人网等。②陌生人交友类：包括遇见、陌陌、兜兜友、友加和夜猫等。③即时通讯类：包括微信、米聊、QQ、Phone +、爱聊免费电话、飞信、私信、YY、Skype 和 Viber 等。

基于位置的应用是移动社交媒体中的典型代表，最容易暴露用户的位置信息，因而对隐私的威胁非常大，也引起了学术界的广泛关注。与传统的桌面社交网络不同，移动社交网络应用将用户的位置信息同实际应用结合在了一起。现有的应用都在用户界面中提供了一张用户当前位置的电子地图，用户不仅可以知道自己所处的位置，而且可以随时发现周围的好友以及获得推荐服务。同时，用户还能将自己刚刚拍的照片、写就的博客发布，发布的内容包含在地图上的某个确切地点，一起与他人分享。这使得移动社交网络应用比传统桌面社交网络更加能够促进同一个地域中人与人之间的交流，因而受到了相当一部分年轻人的喜爱。例如智能手机版的微博、人人网允许用户在使用可定位的移动设备时选择即时更新自己所处的位置（见图 1）。

而陌陌、遇见等陌生人交友类更是充分依赖了位置定位，给人们提供了与附近的人认识的机会。即时通讯类的微信、米聊固然也是基于已有的好友关系（微信基于 QQ 好友，米聊基于通讯录好友）但也增加了附近搜索功能，只要“摇一摇”，就可以发现附近同时使用这一功能的陌生人。

位置信息是一种重要的隐私。首先，位置信息的公开增加了用户被跟踪的威胁。其次，根据连续与重复出现的位置信息的分析可以判断某个用户的工作地点、家庭住址、健康状况等其他隐私。另外，用户隐藏真实位置的自由意愿也因此受到限制。包括位置信息在内，与用户隐私密切相关的信息泄露存在着以下多种途径。

2.2 用户行为引发的隐私泄露

用户可能主动暴露过多隐私。“刷人人”、“晒微博”

图 1　人人网的位置服务 iOS 和 Android 界面截图

等几乎成为移动互联网用户每天的必要活动。而移动社交媒体的即时性、移动性可能会将用户的隐私信息每分每秒都向他人毫无保留地展露出来。根据美国国家消费者报告研究中心的估计，有 480 万人用 Facebook 告诉大家某天要去哪里，这对小偷来说是种非常有用的线索；还有 470 万人“赞”Facebook 平台上某个有关健康状况或者治疗的页面，这些信息都可能被保险推销员利用[18]。

尽管许多社交媒体已经意识到用户隐私泄露带来的问题，并且为用户提供了隐私保护的设置，但是研究表明 Facebook 上很多用户并未使用社交网络提供的这些隐私设置选项，而是将其默认为对所有人开放。大约 1 300 万用户表示，他们从未设置，或者根本就不知道 Facebook 有隐私保护设置。28% 的用户与所有用户（而不仅仅是自己的朋友）分享他们的大部分或是全部内容[18]。

用户在社交媒体填写资料和更新状态主要是基于社交动机。用户希望通过社交媒体与朋友、家人保持联系，也希望通过社交媒体的自动推荐功能找到多年未联系的老朋友，或者发现有共同交际圈与兴趣爱好的新朋友，来扩大自己的交际圈。越加完善的资料越有可能得到更为准确的推荐。

此外也有部分用户将社交媒体空间视为“日记本”，来记录生活中点点滴滴的感受。社交媒体已经成为许多移动互联网用户日常生活不可分割的一部分。因而，可以归纳出用户之所以忽视隐私设置，首先是源于隐私保护意识的缺乏；其次，移动社交应用隐私设置功能的不合理也会成为用户隐私泄露的一大动因。

2.3　服务提供商引发的隐私泄露

从社交媒体的隐私导航功能、关联设置以及隐私设置内容等方面来看，许多社交媒体服务商的隐私功能设置并不合理。

沈洪洲等对朋友网和人人网进行的隐私设置功能的实证研究发现两者均存在不足之处。人人网需要改进其集中式导航方式和集中式导航页面，朋友网则需要改进其分散式导航方式和黑名单功能[9]。

关联设置也是服务商需要改进的重要方面，例如用户可以用自己的 QQ 账户、MSN 账户、新浪微博账户及天翼账户等来登录开心网。QQ 号与开心网账号绑定后，用户在开心网发布的记录和分享内容将被自动同步至腾讯微博及 QQ 空间。不同的社交网站有不同的圈子或者隐私设置，而由于用户忽视关联的存在，很可能造成一些无意的隐私泄露。

好友关系以及群组的隐私设置也被很多社交网络供应商忽视。E. Zheleva 通过分析得出的结论是即使用户设置了最高级的隐私保护，攻击者也可以根据用户所处的群组以及好友关系轻而易举地推断出用户的个人信息[15]。

有的社交媒体服务商收集过多的用户个人信息，这些信息一旦被非法提供给其他组织，或者由于遭受黑客攻击的原因而泄露，便有可能对用户造成巨大的伤害。2010 年底，腾讯 QQ 与奇虎 360 的“弹窗大战”就引发了广大用户对于服务商过多收集个人信息的担忧[19-21]。多数社交网站在隐私声明中均有对用户信息的采集、使用、共享以及 Cookies 的使用。但由于各种网站隐私声明的易读性差，甚至更多的是免责声明，再加上多数社交应用将隐私声明具体内容以链接方式呈现，用户往往忽视其具体内容而直接点击已读同意的按钮，这就有可能在不知不觉间进入了圈套[22-23]。此外，服务商的行为是否涉及过度收集用户信息，在法律上存在漏洞与技术识别难度，使得这一问题更加严峻。

此外，部分网络服务提供商对用户信息的存储并未尽到保障安全的义务。2011 年底，国内知名程序员网站 CSDN 的注册用户信息被黑客盗取，暴露出大量用户口令居然以明文格式保存，可以显示出网站在用户口令保护方面的意识薄弱[24-26]。

2012 年 6 月中国软件评测中心联合北京大学互联网安全技术北京市重点实验室发布了针对国内 100 家网站用户口令处理的安全性测评报告显示：仅有 8 家对用户口令采取了充分安全措施；近六成网站未采取安全措施，导致用户口令直接暴露于服务器及网络之中；甚至有 85 个网站直接拿到了用户口令的原文[27]。可见许多服务提供商对于用户隐私信息保护的意识并不强。

2.4　黑客攻击引发的隐私泄露

黑客攻击是网络犯罪的重要组成部分。具有技术背景的人可以通过网络，在用户不知情的情况下收集其信息。而在移动社交应用中，智能终端的摄像头、耳机等都有可能被有心者“摇身一变”成为监听设备。

J. Franklin 研究了被窃取的个人信息（如被破解的邮箱、身份盗用、信用卡号码等）在地下黑市的商业价值。在该研究中，他们发现了黑客盗取个人信息由出于娱乐的目的到追逐经济利益的驱动力转变[28]。

对于移动社交媒体的用户来说，下载不安全的软件应用或者点击钓鱼链接是遭到攻击最常见的原因。黑客往往通过这些方法获取用户的电脑或者移动终端设备的控制权，并进一步攫取用户的隐私数据、商业机密信息，甚至以用户的终端设备作为跳板，发动进一步的攻击。

3 移动社交网络用户隐私保护综合化方案

上述分析揭示了移动社交媒体用户隐私泄露具有复杂性，因此保护用户隐私需要政府、行业协会、服务提供商以及用户自身等各方面的协同工作（见图 2）。

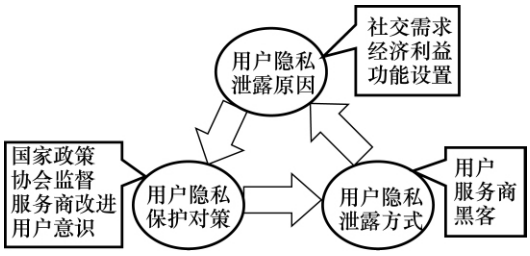

图 2 移动社交网络用户隐私综合化保护方案

从政府层面，制定完善的用户网络隐私保护条例的需求非常迫切。应当明确规定服务提供商在收集、利用用户信息方面应当承担的责任，并且明确对于网络信息犯罪的惩治方式。同时，政府也应当积极以多种途径引导用户提高网络安全意识。

行业协会监督是解决政策相对滞后问题的方法之一。很多国家都采用了这一方式。例如美国著名的网络隐私认证组织 TRUSTe 和 BBBOnline。TRUSTe 是 1996 年由美国电子前线基金会（EFF）与国际商务网（Commerce. net）共同发起成立的以倡导网上隐私保护为主旨的非盈利性机构，对符合隐私保护标准的网站颁发认证证书。BBBOnline 是美国优良商业联合会（Council of Better Business Bureaus）发起的一个计划，旨在通过 BBBOnline 的可靠性和隐私认证，提升用户对国际互联网的信任和信心[10]。申请认证的网站都需要张贴自身的隐私政策公告，并遵守认证机构确定的信息行为规则并服从认证组织的消费者仲裁机制，接受监督和评价。而目前我国此类行业监督机构还比较少。

移动社交网络服务提供商除了接受行业协会监督之外，也应该积极担任起保护用户隐私的责任。随着移动互联网的普及，用户对于移动社交隐私保护也会愈发重视。服务提供商应该在用户信息存储、隐私设置功能以及用户信息安全提醒等方面加大力度。例如提供商还应该承担对用户位置隐私保护的提醒责任。在用户开通位置服务时告知用户哪些程序可以访问位置信息，告知用户上传照片可能会被推断出相关信息的风险，提醒用户谨慎对待陌生人的位置信息请求等。目前，私密型社交网络 Path 在这方面具备优势地位（见图 3）。它称自己为“私人网络”，用户最多只能设置 150 个朋友，基于电子邮件地址和电话号码（而不是用户的公共数据库）分享照片，具有较强的私密性，可以减轻用户对与陌生人分享照片的担心。它的迅速发展足以证明了用户对移动社交网络功能需求的变化。

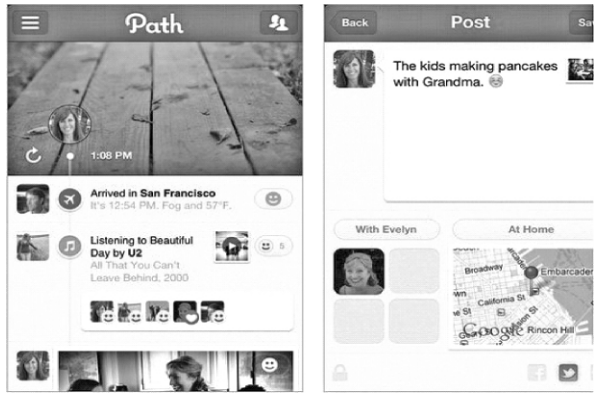

图 3 Path 界面图

用户应当明确各种移动社交媒体的不同之处，区别各个社交媒体的不同“好友”关系。应该有选择性地发布信息、更新状态，选择较高级别的隐私设置，选用安全性较高的应用程序，安装移动终端杀毒软件，定期查杀病毒，查询费用记录等。

4 结论与展望

本文讨论了在移动互联网背景下，社交媒体用户隐私泄露的方式、原因并结合多种类型主体，提出了综合化的解决方案。传统的网络隐私保护趋向于阻止用户发布信息，而这种方式在移动社交网络中并不可取，因为用户加入社交网络的目的就在于参加社交活动。

由于受到道德法则的约束，本研究提出的解决方案无法采用实验与实践方法进行验证，因为有可能暴露或者侵犯用户隐私权。在未来可以尝试利用复杂系统仿真技术等手段，在不侵犯现实生活中用户隐私的前提下进行验证。

移动互联社交应用是未来社交的发展趋势，开发用户友好型的社交网络应用并提供功能合理的隐私设置是移动社交网络用户隐私保护的关键内容，因而值得进一步深入研究。□

参考文献

[1] GANNES L. Mary meeker explains the mobile monetization challenge-liz gannes-D10-allThingsD [EB/OL]. [2012-11-06]. http://allthingsd.com/20120530/mary-meeker-explains-the-mobile-monetization-challenge/?mod=googlenews_editors_picks.

[2] CNNIC. 第30次中国互联网络发展状况统计报告 [EB/OL]. [2012-11-06]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201207/t20120723_32497.htm.

[3] 秦川. 网络犯罪转向社交网络和移动终端 [EB/OL]. [2012-11-06]. http://newspaper.jfdaily.com/xwwb/html/2012-10/14/content_898263.htm.

[4] WU Zhenyu, ZHANG Chunhong, JI Yang, et al. Towards cloud and terminal collaborative mobile social network service [C]. Social Computing (SocialCom), 2010 IEEE Second International Conference, 2010.

[5] LIN S W, LIU Y C. The effects of motivations, trust, and privacy concern in social networking [J]. Service Business, 2012, 6(4): 1-14.

[6] 胡磊. 试论网络隐私权的隐私范围及其保护——从"Google Earth"事件说开去 [J]. 情报资料工作, 2007(3): 58-61.

[7] 魏来, 郑跃. 隐私2.0: Web2.0时代的用户隐私保护研究 [J]. 图书与情报, 2010(5): 60-64.

[8] 孙剑, 朱晓妍, 刘沫盟, 等. 社交网络中的安全隐私问题研究 [J]. 网络安全技术与应用, 2011(10): 76-79.

[9] 沈洪洲, 宗乾进, 袁勤俭, 等. 我国社交网络隐私控制功能的可用性研究 [J]. 计算机应用, 2012(3): 690-693.

[10] 刘颖. 论个性化信息服务中的隐私保护 [J]. 情报科学, 2007(12): 1794-1798.

[11] HOY M G, MILNE G. Gender differences in privacy-related measures for young adult Facebook users [J]. Journal of Interactive Advertising, 2010, 10(2): 28-45.

[12] GROSS R, ACQUISTI A. Information revelation and privacy in online social networks [C]//Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 2005.

[13] LUO B, LEE D. On protecting private information in social networks: a proposal: data engineering [C]. ICDE'09. IEEE 25th International Conference on, 2009.

[14] ZHELEVA E, GETOOR L. Preserving the privacy of sensitive relationships in graph data [C]//Proceeding of Privacy, Security, and Trust in KDD workshop, 2008: 153-171.

[15] ZHELEVA E, GETOOR L. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles [C]//Proceedings of the 18th International Conference on World Wide Web, 2009.

[16] ARDAGNA C A, CREMONINI M, et al. An obfuscation-based approach for protecting location privacy [J]. Dependable and Secure Computing, IEEE Transactions on, 2011, 8(1): 13-27.

[17] WANG Wendong, et al. Sharing information with controllable precision by distance measuring in mobile social network [C]. Wireless Communications, Networking and Mobile Computing, 2009. WiCom09. 5th International Conference on, 2009.

[18] MAGAZINE C R. Facebook & your privacy who sees the data you share on the biggest social network? [EB/OL]. [2012-11-07]. http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm.

[19] 袁茵. 3Q大战未了局 [J]. 中国企业家, 2012(9): 77-79.

[20] 李萧然, 李琳. 3Q大战续集: 一起过程比结局更精彩的悬案 [J]. IT时代周刊, 2012(9): 30-36.

[21] 魏雅华. 解读3Q大战 [J]. 企业研究, 2010(23): 10-13.

[22] 周涛. 基于内容分析法的网站隐私声明研究 [J]. 杭州电子科技大学学报: 社科版, 2009(3): 11-16.

[23] 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.

[24] 岳逍远. "CSDN泄密门"事件两名涉案黑客已落网 [J]. 信息网络安全, 2012(2): 94.

[25] 张耀辉. CSDN"拖库"事件后对密码保护的反思 [J]. 长沙通信职业技术学院学报, 2012(2): 37-40.

[26] 仝磊. 由CSDN信息泄露事件引发的思考 [J]. 网络安全技术与应用, 2012(2): 7.

[27] 周静. 九成网站未充分保护用户密码 网民隐私竟成盘中餐: 全景财经新闻频道 [EB/OL]. [2012-11-07]. http://www.p5w.net/news/cjxw/201206/t4313206.htm.

[28] FRANKLIN J, PAXSON V, PERRIG A, et al. An inquiry into the nature and causes of the wealth of internet miscreants [C]. ACM Conference on Computer and Communications Security (CCS), 2007.

作者简介: 王树义, 男, 1982年生, 讲师, 博士。研究方向: 信息管理和信息系统。

朱娜, 女, 1987年生, 硕士生。研究方向: 知识管理与竞争情报。

收稿日期: 2012-12-25