再谈 Facebook 事件与在线社交网络隐私保护

陈 阳 宫庆媛 王 新
复旦大学

关键词：在线社交网络 隐私泄露 隐私保护

在线社交网络已经成为了主流的互联网应用，国外的 Facebook、Twitter、LinkedIn 以及国内的微信、微博、人人网等社交平台吸引了数十亿互联网用户。作为人们日常生活的重要组成部分，在线社交网络在社会经济发展中起着越来越重要的作用。在服务广大用户的同时，这些网站也记录了海量的用户行为数据，包括涉及个人隐私的敏感数据。随着在线社交网络的快速发展和广泛覆盖，在线社交网络的隐私保护也成为了一个有现实意义的重要课题。

2018 年 3 月，全球最大的在线社交网站 Facebook 卷入了一起大量用户隐私泄露的事件。这批数据泄露的渠道是 Facebook 网站对第三方应用所提供的 Graph API。开发者可以基于这套 API 编写应用程序吸引用户使用，通过用户的授权，获取使用了该应用程序的用户的基本信息。在此基础上，该应用程序还可以基于每个用户的社交关系，进一步收集其好友的信息[1]。最终，在这一事件中，多达数千万用户的行为数据在不知情的情况下被获取。该事件也在全世界范围内引发了针对在线社交网络用户隐私保护的诸多关注与讨论。

在线社交网络的隐私泄露

内容发布是在线社交网络的核心功能。用户生成内容 (User-Generated Contents, UGC) 经由社交网络进行广泛传播，也引入了隐私泄露的风险。主流在线社交网络几乎都支持图片发布与分享服务，用户常常将生活中的照片发布到社交网络上，这些照片可能包含用户自己和朋友的形象。Facebook 等社交网络还允许图片的发布者将发布的图片中所包含的 Facebook 用户标记出来，称为“圈人 (tag)”。希腊研究与技术基金会的 Ilia 等学者[1]发现，在以 Facebook 为代表的在线社交网络中，用户可以任意发布包含他人的图片而不需要得到图片中其他人物的同意，发布者甚至可以将图片的访问权限设置为“所有用户可见”。除发布者以外，图片中的其他用户并没有相应的渠道对此进行限制，也就无法制止自己的形象在社交网络上传播。而且，Facebook 等社交网络也没有对图片发布者提供足够的激励或提醒以保护图片中人物的隐私。因此，涉及用户隐私的图片可能通过社交网络得到传播。例如，当前许多父母喜欢将自己孩子的照片在社交网络中发布并分享，这也对儿童的隐私保护带来了挑战。美国纽约大学的 Minkus 等学者[2]分析了 2383 位 Facebook 成年用户和 1089 位 Instagram 成年用户的公开相册，发现有 34.8% 的 Facebook 用户和 100% 的 Ins-

[1] Facebook 于 2015 年 4 月 30 日关闭了 1.0 版本的 Graph API，在此之后对用户信息获取有了更严格的限制。

tagram 用户发布过至少一张儿童照片。作者还发现，利用图片的评论信息，可以获取照片中儿童的姓名、生日和地址等信息。因此，关于儿童的许多信息可能被父母在不经意间泄露，造成潜在的危险。

随着智能手机、平板电脑等移动设备的普及，在线社交网络也提供了一系列基于位置的社交服务并记录了大量的用户时空信息。用户可以在发布的帖子中添加位置信息，也可以利用“发现附近的人”等功能，查看周边用户的信息。基于位置的服务在提供给用户许多方便的同时，也带来了一些风险，例如实时位置信息的泄露。攻击者可以伪装成正常用户，并伪造自己的所在位置，发现该位置周边用户的相关信息。另外，攻击者可以从多个不同的预设地点发送请求，获取与目标用户的多个相对距离，求解计算目标用户的位置。移动社交网络通常会对位置或距离的相关请求返回近似值而不是精确值，以避免攻击者利用这些功能获取目标用户的准确位置。美国哥伦比亚大学的 Polakis 等学者 [3] 就移动社交网络用户位置信息泄露问题进行了研究。作者研究了攻击者利用移动社交网络提供的信息、通过多轮查询获取用户实际位置的过程。作者针对不同场景提出了经过优化的攻击算法，分析得到了攻击者为获取目标用户的准确位置所需要的查询次数的下界。作者选取了 Facebook、Foursquare/Swarm、Grindr 和 Skout 这四个有代表性的移动社交网络进行了实验。结果表明，尽管移动社交服务对用户之间的距离测量进行了一定的模糊化处理，攻击者仍然可以利用有限的查询次数，准确地推断出目标用户的位置信息。

当前一个用户往往在多个社交网络上拥有自己的账号，以使用不同的社交网络服务。不同的在线社交网络要求用户提供的信息不尽相同，用户倾向于根据自己的使用目的和相应社交网络的功能，在不同社交网络上填写或发布不同层面的信息。我们注意到，大部分新兴社交网络提供了“跨网站链接”(cross-site linking) 这一服务功能 [4]，支持用户将其在该网站上的账号和在主流社交网络如 Facebook、Twitter 等网站上的账号进行跨站链接。一方面，这一功能大大方便了用户使用社交网络服务，包括跨站发帖、好友关系导入以及更全面的自我展示。另一方面，这一功能也带来了隐私泄露的风险。攻击者有机会聚合用户的多方面信息，并对用户公开发布的内容进行跨网站汇总，从而重构出用户详尽的行为信息。根据我们对 Foursquare 网站用户的测量分析，有超过一半的用户选择了使用该功能，链接自己在其他社交网络上的账号。攻击者通过访问用户在某一社交网络的主页，可以直接跳转到用户在其他多个社交网络上的主页，从而获取并汇总其在不同网站的信息。 同时，也有部分用户出于对个人隐私的保护，选择不使用跨站链接功能，避免直接公开自己在多个社交网络上的账号。然而，这一做法也无法确保用户的隐私得到全面的保护。有许多研究工作通过不同社交网络账号上的用户行为数据，成功匹配出多个不同网站的账号属于同一个用户。卡内基梅隆大学的 Liu 等学者 [5] 利用了用户在不同社交网络行为的相似性，提出了多社交网络用户账号匹配系统 HYDRA。基于新浪微博、腾讯微博、人人网、豆瓣和开心网，以及 Twitter 和 Facebook 用户数据的实验结果表明，HYDRA 可以高效准确地发现在这些社交网络上属于同一用户的账号。

在线社交网络隐私保护措施

鉴于用户隐私保护的重要性，不少研究人员也提出了一系列在线社交网络隐私保护措施，这些措施一方面能够对现有在线社交网络平台存在的隐私泄露风险进行防范，另一方面能够保证用户仍然有较好的社交服务使用体验。

希腊研究与技术基金会的 Ilia 等学者 [1] 研究了社交网络中图片的访问控制问题。为了解决这一问题，作者提出了一套新的访问控制模型，将访问控制的粒度由每一张图片细化到图片中的每一个人物，即图片中的每一个人物而不是图片上传者作为隐私权限设置的主体。这一模型以人脸识别技术为基础，对于上传的图片，平台将对其包含的人脸进

行识别，并和网络中已有用户进行比对。当包含某一用户的图片被上传后，平台将通知该用户，并由其进行访问权限控制。在得到该用户的明确允许之前，平台将会暂时对图片中该用户的人脸进行模糊处理，从而保护用户隐私。

谷歌公司的 Bilogrevic 等学者 [6] 研究了移动社交网络中，模糊化处理“签到”的地理位置信息对于服务可用性 (utility) 的影响，探讨了用户隐私保护和服务可用性之间的权衡 (trade-off) 问题。作者首先研究了用户使用签到功能的动机，利用亚马逊土耳其机器人 (Amazon Mechanical Turk) 平台，招募了 77 位 Foursquare 的活跃用户进行有偿调研并通过问卷获取了这些用户每次签到的首要和第二位的目的。同时，作者进一步了解了当对签到信息进行一定程度的模糊化时，用户是否认为模糊化后的签到信息还可以达到其进行该次签到的目的。分析结果表明，基于语义的模糊化 (semantic obfuscation) 对服务可用性的负面影响要显著大于基于地理位置信息的模糊化 (geographic obfuscation)。作者构建了一套基于监督式机器学习的模型，可以较准确地预测签到的目的 (准确率是 baseline 算法的两倍)。进一步，根据预测的签到目的，对用户的签到信息，提出相应的不同程度的模糊化措施。这一方案可以达到用户隐私保护和服务可用性的较好平衡。

美国普林斯顿大学的 Liu 等学者 [7] 设计了 LinkMirage 系统，该系统通过对社交关系图的边进行扰动 (perturbation)，即匿名化处理，可以得到一个既能保持原图的结构属性、又能保护用户隐私的新图。这一系统不仅适用于静态的社交关系图，还能对演化中的社交关系图进行处理。利用一台普通的计算机工作站 (3.6GHz CPU，24GB 内存)，LinkMirage 系统可以在 100 秒内处理包含 9.4 亿条边的社交关系图。作者通过实验表明，经过 LinkMirage 系统处理的社交关系图具有和原图非常接近的 PageRank 值和模块度 (modularity)。这一系统可以支持基于隐私保护的图分析、匿名通信以及恶意账户检测等问题的研究。

未来研究趋势

- 用户体验与隐私保护的平衡。目前的一些以牺牲用户隐私为代价的社交网络功能将会被更可靠同时又能保证可用性的功能所取代。
- 帮助广大用户特别是非专业用户灵活地进行细粒度的隐私权限配置，方便而准确地控制信息的传播范围。
- 保障用户隐私前提下的大数据分析。在线社交网络提供了海量的用户行为数据，将来的研究将会更好地保证在利用社交大数据进行分析的同时不侵犯个体用户的隐私。 ■

陈　阳

CCF 专业会员，CCF 互联网专委会委员。IEEE 高级会员。复旦大学计算机学院副教授。主要研究方向为互联网体系结构、社交网络、移动计算等。
chenyang@fudan.edu.cn

宫庆媛

CCF 学生会员。复旦大学计算机学院博士生。主要研究方向为在线社交网络、用户行为分析、机器学习等。
gongqingyuan@fudan.edu.cn

王　新

CCF 杰出会员，CCF 互联网专委会副主任。复旦大学计算机学院教授。主要研究方向为新一代互联网体系结构、无线与移动网络、数据中心网络、网络存储系统等。
xinw@fudan.edu.cn

参考文献

[1] Ilia P, Polakis I, Athanasopoulos E, et al. Face/Off: Preventing Privacy Leakage From Photos in Social Networks[C]//*Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015:781-792.

[2] Minkus T, Liu K, Ross K W. Children Seen But Not Heard: When Parents Compromise Children's Online Privacy[C]// *Proceedings of the 24th International Conference on World Wide Web*, 2015:776-786.

[3] Polakis I, Argyros G, Petsios T, et al. Where's Wally?:Precise User Discovery Attacks in Location Proximity Services[C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015:817-828.

[4] Gong Q, Chen Y, Hu J, et al. Understanding Cross-site Linking in Online Social Networks[J]// To appear: ACM Transactions on the Web (TWEB).

[5] Liu S, Wang S, Zhu F, et al. HYDRA: large-scale social identity linkage via heterogeneous behavior modeling[C]// Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data. ACM, 2014:51-62.

[6] Bilogrevic I, Huguenin K, Mihaila S, et al. Predicting Users' Motivations behind Location Check-Ins and Utility Implications of Privacy Protection Mechanisms[C]//Proceedings of the Network & Distributed System Security Symposium, 2015.

[7] Liu C, Mittal P. LinkMirage: Enabling Privacy-preserving Analytics on Social Relationships[C]//Proceedings of the Network & Distributed System Security Symposium, 2016.