

大数据背景下医学生移动社交网络个人信息泄露及保护策略研究^{*}

张荣兴 杨玉赫 冷德生

(黑龙江中医药大学 哈尔滨 150040)

〔摘要〕 分析大数据背景下移动社交网络特征,对移动社交网络中医学生个人信息泄露现状、原因以及个人信息保护策略进行研究,包括建立健全相关法律体系、提高医学生信息安全意识等方面,为医学生网络信息安全教育提供参考。

〔关键词〕 大数据;医学生;移动社交;个人信息;保护策略

〔中图分类号〕 R-056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2020.01.006

Study on Personal Information Leakage and Protection Strategy of Medical Students on Mobile Social Network under the Background of Big Data ZHANG Rongxing, YANG Yuhe, LENG Desheng, Heilongjiang University of Chinese Medicine, Harbin 150040, China

〔Abstract〕 The paper analyzes the characteristics of mobile social network under the background of big data, studies the current situation and causes of medical students' personal information leakage on mobile social network as well as personal information protection strategy, including establishing and improving relevant legal systems, enhancing medical students' information security awareness, etc., providing references network for information security education of medical students.

〔Keywords〕 big data; medical students; mobile social; personal information; protection strategy

1 引言

如今移动社交网络所形成的虚拟空间和现实生活已达到高度的重合,不但促进医学生用户群体间的互动交流,也增加个人信息泄露的风险。与此同

时相关企业基于移动社交网络所产生的商业价值,对医学生用户个人信息不断进行挖掘与利用,从而造成用户隐私泄露。用户个人信息安全的保护问题将成为影响移动社交网络行业稳定发展的重要因素之一。

2 大数据背景下移动社交网络特征

2.1 大数据时代的主要特征

规模大,人们时时刻刻都在智能终端上产生大量数据^[1];具有强大的时效性,需要快速存储和处理;表达形式多种多样,既包括文字类结构化的数据,也有图片、音频、视频等其他非结构化的数据

〔收稿日期〕 2019-06-13

〔作者简介〕 张荣兴,硕士,讲师,发表论文 15 篇;通讯作者:冷德生,副教授。

〔基金项目〕 教育部产学研协同育人项目“大学生创新创业教育通识课程《自我发展与创业指导》研究与实践”(项目编号:201802165020)

形式。在移动社交网络中的数据多以非结构化为主^[2]。

2.2 大数据时代的移动社交网络

移动社交网络在大数据蓬勃发展的背景下面临新的机遇和挑战并不断呈现出新的特点。首先,社交网络上非结构化信息日益增多,在为用户提供全新的交流互动体验的同时也在社交网络上透露更多的个人真实信息^[3]。其次,移动地理位置信息分享应用日渐风靡,用户的信息资源作为其主要内容之一,在移动社交网络中的安全性越发重要。

2.3 医学生使用移动社交网络的特点

医学生在移动社交网络上主要以手机、平板等移动智能终端为载体,以智能终端在线识别以及交换信息技术为基础,具有人机交互、实时场景等特点,能够随时随地创造并分享信息,让网络最大程度地服务于现实生活。移动社交网络沿袭传统社交网络内容与传播形式的多样化、互动性极强等特点,也由移动化、本地化、社交化 3 个核心特征衍生出一些新的特点。第一,基于活动与情景。如医学生使用签到功能只是表明一个人已登录,此外并没有获得更多的服务。第二,在移动社交平台只需打开手机的移动网络就能接收到各种医学相关信息。

3 移动社交网络中医学生个人信息泄露现状

3.1 获取服务泄露基本信息

移动社交网络中医学生的基本信息是其在注册相关账号时所提供的个人情况,这些信息是其获取部分服务的基础。移动社交应用往往需要用户提供较为完整的个人信息从而达到提供个性化服务的目的,如果医学生用户填写虚假信息会影响其使用社交应用功能以及使用效果。目前大多数移动社交应用都需要通过激活或者手机验证码的形式获取医学生用户的个人有效信息,容易导致医学生手机号码、电子邮箱等通讯信息的泄露。

3.2 精准定位泄露位置信息

移动社交网络中移动位置信息的引入提高了医学信息传播真实性,同时也增加了医学生个人隐私泄露的风险。由于终端体验十分丰富,微信、腾讯 QQ 等社交软件还支持用户通过位置信息的共享实现陌生人交友的不同体验。移动社交定位基于医学生社交与移动两方面的特征而实现,与单纯的位置服务 APP 相较而言更容易暴露医学生个人隐私,精准定位极大影响医学生人身和财产安全。通过医学生位置信息出现的频率及其相关社交信息,易检测出如家庭住址、工作地点、经常活动地址信息等,增加医学生在现实生活中遇到危险的风险。

3.3 移动服务泄露轨迹信息

移动社交基于智能终端与互联网络的移动性而增加用户个人隐私暴露的风险。轨迹信息不仅仅指用户上网的轨迹数据,还指在移动性的基础上通过用户多次位置信息而构成的一种特制的专属位置信息。目前医学生通过移动终端系统进行间断性定位的现象越来越常见。医学生的移动轨迹大多呈三点一线规律性,容易泄露医学生日常生活信息。

3.4 社交应用泄露社会关系信息

随着移动社交网络的不断深入,医学生的社会关系网越来越清晰地显现出来,攻击者不需要很高的技术就可以攻破医学生社会关系网。目前移动社交主要为医学生提供两种不同的互动平台:开放式与半开放式。开放式互动平台如腾讯 QQ,容易获取并利用医学生社会关系信息。半开放式互动平台如微信,较开放式平台稍有进步,但仍存在医学生社会关系隐私信息泄露的危险。此外医学生还面临黑客攻击、社交网络运营商对于信息的收集与利用等方面的泄露风险。

4 医学生移动社交网络中个人信息泄露原因

4.1 社会层面

4.1.1 基于真实性的移动社交环境诱导医学生用

户泄露信息 医学生在社交网络中所形成的人际关系能够为其提供最大限度的信任感。而信任感的产生主要表现为两个方面：一方面是指群体规范下的自我揭露行为；另一方面是指信任的转移，即通过已经取得信任的个体将其所获取的信任感转移到他人所信任的个体上。移动社交网络与传统社交网络相比引入了更多真实性因素，通过鼓励用户进行实名制注册以及开展自我揭露行为从而不断收集用户手机号码、地理位置等真实信息，为用户创造与现实社交环境高度吻合的网络社交环境。具有真实性的移动社交环境虽然能够提高医学生间信息交流与传播速度和效率，但也容易使其放松警惕，忽视对个人隐私信息的保护。

4.1.2 基于开放性的移动社交环境容易泄露医学生用户隐私 主要表现在网络以及平台的开放，网络的开放主要是指准入门槛的开放。仅需智能终端、移动互联网络和相关社交 APP，任何人都可以成为移动社交网络用户并享受相关的一切体验服务。平台的开放主要是指第 3 方平台的介入。目前移动社交应用基本实现不同应用的互登、关联、分享等一系列功能，以满足服务商对用户信息的需求量，从而增强用户网络黏度。医学生通常会在社交群体中揭露个人隐私信息，但账号互登、关联等功能容易使其忽略情景的差异而造成个人隐私的泄露。

4.2 用户自身因素

大数据背景下个人隐私泄露的案例时常发生。当医学生最初开始使用某些社交 APP 时需按要求填写个人基本信息，此时信息已被开发商收集^[4]，当黑客入侵个人信息存储系统时极易造成信息泄露。此外医学生浏览网页时若触及有木马病毒的网页，也会导致医学生个人信息的泄漏^[1]。在以用户为中心的社交网络环境中，用户自身行为与隐私意识是关键因素，隐私保护意识薄弱、乐观的隐私态度等都可能产生影响。

4.3 服务商

目前医学生隐私泄露与部分服务商所提供的不

恰当功能体验存在密切联系。医学生可以在众多 APP 上发现不少应用隐私功能设置都需要多重连接才能完成。各社交 APP 使用之初的默认状态都是最大化地暴露用户个人信息，若不提前设置访问权限各类社交 APP 的可视范围都是所有人可见。此外隐私保护政策存在过度形式化问题。默认“已阅读”形式致使医学生对隐私政策的陌生，而且这些政策对于隐私保护的可实施性较差。综上所述，诸如此类不合理的设置无一不在弱化医学生的隐私保护。

4.4 国家法律

法律法规不够完善造成医学生隐私保护无法可依。国内隐私保护法律法规不健全加大网络环境用户隐私的保护难度。目前在我国隐私权还未被列为独立人格权加以保护，我国宪法及民法对于人格权、名誉权的规定仅具有框架性，缺乏较为系统的描述。而网络隐私保护更缺少相关法律法规，目前仅依靠一些零散、不成文的行政法规。

5 医学生移动社交网络个人信息保护策略

5.1 政府建立健全移动社交网络个人信息保护法律体系

大数据作为新生事物，存在相关法律法规缺失、无法有效维护用户个人信息安全等问题。《网络安全法》于 2017 年正式实施，个人信息保护被纳入重点保护范围，对于隐私条款有着更为具体的要求。随着隐私政策的相继更新，在网络社交等各方面规范服务商对用户信息的使用。

5.2 提高医学生用户信息安全意识

大数据背景下保护医学生个人信息安全最有效的办法是提高其信息安全素养。丰富的信息安全知识有利于医学生了解、辨识木马、钓鱼等网站，由此提高自身信息安全保护意识。提高信息安全素养应从以下方面着手：首先要有节制意识。理性地应用移动社交网络，有效设置访问权限，将个人信息放置在安全范围内。其次提高账户信息安全设置等

(下转第 39 页)

- 3 杨林, 李姣, 侯丽, 等. 跨领域数据审编 (Curation) 流程研究——以环境健康数据为例 [J]. 现代图书情报技术, 2016, 31 (12): 80–88.
- 4 Poux S, Arighi C N, Magrane M, et al. On Expert Curation and Scalability: UniProtKB/Swiss – Prot as a case study [J]. Bioinformatics, 2017, 33 (21): 3454–3460.
- 5 Dauga D. Biocuration: a new challenge for the tunicate community [J]. Genesis, 2015, 53 (1): 132–142.
- 6 International Society for Biocuration. Biocuration: distilling data into knowledge [J]. PLoS Biology, 2018, 16 (4): e2002846.
- 7 Orchard S, Kerrien S, Abbani S, et al. Protein Interaction Data Curation: the International Molecular Exchange (IM-Ex) consortium [J]. Nature Methods, 2012, 9 (4): 345.
- 8 Zhang Z, Sang J, Ma L, et al. RiceWiki: a wiki – based database for community curation of rice genes [J]. Nucleic Acids Research, 2014, 42 (D1): 1222–1228.
- 9 Howe D, Costanzo M, Fey P, et al. Big data: the future of biocuration [J]. Nature, 2008, 455 (7209): 47.
- 10 Van Auken K, Fey P, Berardini T Z, et al. Text Mining in

- the Biocuration Workflow: applications for literature curation at WormBase, dictyBase and TAIR [J]. Database, 2012 (2012): 1–13.
- 11 ClinGen. Clinical Laboratories Meeting Minimum Requirements for Data Sharing to Support Quality Assurance [EB/OL]. [2019–01–10]. <https://www.clinicalgenome.org/lablist/>.
- 12 Strande N T, Riggs E R, Buchanan A H, et al. Evaluating the Clinical Validity of Gene – disease Associations: an evidence – based framework developed by the Clinical Genome Resource [J]. The American Journal of Human Genetics, 2017, 100 (6): 895–906.
- 13 Griffith M, Spies N C, Krysiak K, et al. CIViC is a Community Knowledgebase for Expert Crowdsourcing the Clinical Interpretation of Variants in Cancer [J]. Nature Genetics, 2017, 49 (2): 170.
- 14 Villaveces J M, Jimenez R C, Porras P, et al. Merging and Scoring Molecular Interactions Utilising Existing Community Standards: tools, use – cases and a case study [J]. Database, 2015 (2015): 1–12.

(上接第 33 页)

级。医学生应尽可能避免使用本人姓名的拼音、缩写或生日等方式来申请和设置社交网络账户密码,减少用同一密码申请多个 APP 应用的情况,同时还应避免传送个人网络账号密码等。最后主动接受信息安全教育。研究表明接受过信息安全培训的医学生具有信较强的信息安全意识,也有较好的个人信息保护能力^[5]。

5.3 大数据服务商应改善移动社交网络的安全性

良好的行业规范和自律公约是一个行业蓬勃发展的重要条件。大数据服务商应加强行业自律,规范企业行为,提高准入标准,做好成员资质审核。此外要积极创新,优化网络结构,做好信息保护,规范数据采集行为,保证用户个人信息的安全和自由。

6 结语

大数据是当前信息产业发展的基础,也是其未来发展的重要方向,做好大数据的技术研究对于提

高信息技术质量具有十分重要的作用。而在这一过程中怎样应对医学生个人隐私信息安全所面临的挑战成为重要研究内容。这一研究的开展不但有助于大数据背景下医学生网络信息安全性的提高,也为大数据技术提供更为广阔的发展空间。

参考文献

- 1 吴静梅. 大数据下大学生移动社交网络个人信息保护研究 [J]. 智库时代, 2018 (45): 208–209.
- 2 封二英, 齐晓娜, 张宇敬. 大数据下大学生移动社交网络个人信息保护研究 [J]. 产业与科技论坛, 2018, 17 (1): 39–40.
- 3 殷国伟. 网络环境下高校学生个人信息资料的法律保护 [J]. 湖州师范学院学报, 2009, 31 (3): 73–77.
- 4 维克托·迈尔·舍恩伯格, 肯尼思·库克耶. 大数据时代: 生活, 工作与思维的大变革 [M]. 杭州: 浙江人民出版社, 2012.
- 5 王来兵. 大数据时代社交网络个人信息安全问题研究 [J]. 赤峰学院学报 (自然版), 2017, 33 (13): 19–20.