Social Media in Health Care: Time for Transparent Privacy Policies and Consent for Data Use and Disclosure

Carolyn Petersen[1] Christoph U. Lehmann[2]

[1] Global Business Solutions, Mayo Clinic, Rochester, Minnesota, United States
[2] Departments of Biomedical Informatics and Pediatrics, Vanderbilt University, Nashville, Tennessee, United States

Address for correspondence Carolyn Petersen, MS, MBI, FAMIA, Global Business Solutions, Mayo Clinic, 200 First Street SW, Rochester, MN 55905, United States (e-mail: petersen.carolyn@mayo.edu).

Appl Clin Inform 2018;9:856–859.

Social media has taken its place within health care. The digital health movement promoted social media as a collaboration between patients, their caregivers, medical professionals, and other stakeholders in health.[1] Social media introduces people to health information and health-preserving practices, connects patients and caregivers (who share common challenges), and provides an anonymous space for individuals for exploration of health concerns that could otherwise be stigmatizing. Social media allows patients and relatives to crowdfund expensive treatments and research their disease or encourage others to become donors for organ or bone marrow transplants. However, even as social media platforms provide dedicated spaces for health-focused users and user groups, platforms frequently fail to take into account the unique needs of this population, which can create special challenges and additional work for health care practitioners and may require focused efforts to overcome real and potential privacy abuses. Even more disquieting, social media information may provide manipulated and false content[2] as well as a false sense of privacy, as demonstrated by the finding that Facebook data can be used to predict personal attributes such as ethnicity, sexual orientation, and substance use[3] and by the widely publicized Facebook–Cambridge Analytica breach.[4]

With the use of social media increasing (~70% in North America, 66% in Northern Europe, 64% in East Asia, and 63% in South America), sharing your own details, even deeply personal, intimate information through social media, has become a routine part of life for many.[5] Users share information for various reasons, and in so doing may also fulfill broader societal objectives such as introduction and testing of new ideas. As continuous self-distribution of protected health information becomes the predominant standard,[6,7] this surveillance capability may evolve from an authoritarian function to what Pecora has termed "a populist path to self-affirmation."[8] Given the ubiquity of online patient communities organized around Facebook, Twitter, and other platforms, some might argue that this shift has already occurred and that patients, who use social media to find others with like interests, have created a standard for interaction in health care.

As with relationships between providers and patients, the use of social media to connect with others who share similar health needs and interests is based upon trust.[9] In social media, this trust encompasses many dimensions: trust in the Internet service provider not to snoop, trust that the platform will be operated as described in the terms of use, trust that others will follow the rules of conduct, trust that others will portray themselves and their activities on the site accurately, and trust that community members will share information appropriately.[10,11] Although most users recognize that there can be no absolute guarantee that others will act in accordance with the group's rules, they also anticipate that breaches of the agreement will be infrequent and minor in scope.

Facebook has a decade-long history of acting against the user expectations it shaped via its privacy policy and marketing messages. Facebook is still facing action by the U.S. Federal Trade Commission resulting from several data breaches and the scraping of data from 2.2 billion users that violated a 2011 consent decree on user privacy.[12] The investigation failed to deter the platform from pursuing unclear and even deceptive data sharing activity.[13] The recent revelations about Facebook's handling of user information have confirmed suspicions that an industry offering its services for free to users most likely has already turned its user base into the marketed product or is about to do so. More importantly, such revelations leave individuals who use social media feeling betrayed, bereft, violated, and concerned about how to safely and appropriately use social media to support health-related goals and build community.[14,15]

Facebook's engagement of a physician to seek covert deals with health care organizations for sharing of patients' protected health information was directly at odds with patients'

received
August 1, 2018
accepted after revision
October 25, 2018

DOI https://doi.org/10.1055/s-0038-1676332.
ISSN 1869-0327.

expectations of confidentiality for their health information.[16] Though aggregation of information shared via Facebook with electronic health record data could provide insight for care providers seeking to improve patients' health, the creation and sharing of enhanced patient profiles are precariously left open to unlawful sharing of personal information, even social stigma and discrimination.[17]

Facebook further alienated users when it failed to protect information shared by users who signed up for private groups, which in some cases are organized around health issues or shared experiences. Until mid-2018, Facebook permitted third parties to scrape user-generated health information from private groups for nonsupport-group uses.[18] The design and management of Facebook's Groups functionality has facilitated other negative consequences for private group users. Allowing hostile nonmembers to take over a private group used by survivors of rape and sexual abuse not only validated members' concerns about being exposed publicly, but also retraumatized members.[19] Facebook's privacy policy and technology also permitted rehabilitation of clinic marketers to target members of the private group Affected by Addiction Support Group.[20] In addition, many users were concerned when it became apparent that not only their own data but also the data of friends were shared. Inadvertently, Facebook users had betrayed the trust of others.[21]

Even users who are unaffected by Facebook's handling of private groups employ strategies to limit unwanted sharing of personal information. Users employ techniques that are preventive (e.g., signing up with false identities, managing friend lists to avoid sharing information with particular people), corrective (e.g., untagging), information control (e.g., self-censorship), and collaborative (i.e., comanaging with others the posting of information) strategies to avoid exposing personal information to people with whom they do not wish to share it.[22,23] Some might argue that the practice of these evading strategies indicate that users understand and accept the limitations of privacy on social media platforms. However, use of privacy management strategies by individuals who lack local support for health-related needs (e.g., those with rare conditions, people who lack transportation to support groups, rural residents, those who have stigmatizing conditions, etc.) may reflect a forced tolerance rather than a warm embrace.

Though Facebook's transgressions are perhaps the highest profile to date, the problems that have come to light on Facebook could occur on other social media platforms, and Facebook is hardly the only pain point for users. The Children's Online Privacy Protection Act, one of the more progressive laws covering Americans' personal information, stipulates data collection practices that are prohibited or require parental consent for users below 13 years. However, analysis of 5,855 of the most popular free apps aimed at children revealed that a majority failed to adequately disable tracking and behavioral advertising.[24] Even more concerning, 19% of the apps use software development kits expressly prohibited for use in children's apps because they collect personally identifiable information. Americans are trained early to expect and tolerate illegal collection and distribution of personal information.

It is tempting to think that data misuse can be ignored because breaches of privacy and confidentiality have been happening since the beginning of digital health care, and developers have yet to experience a significant backlash with patients fighting for their right to privacy. Rather, now is the time to proactively address privacy-related issues so that sources of patient-generated health data that hold promise for improved outcomes (e.g., electronic patient-reported outcome measures, wearables, remote sensors) remain acceptable to patients now and in the future.

Creating a transparent environment in which social media platforms afford users the desired opportunities alongside known, manageable risks requires a twofold approach: a comprehensive consumer education campaign along with robust laws that motivate platform operators to implement user-friendly business models and policies. Public health campaigns focused on smoking cessation, seat belt use, and other health-enhancing behaviors have reduced unhealthy-harming behavior and improved health outcomes.[25–27] The principles on which these campaigns were built (e.g., clear language, succinct messaging) may form the basis for initiatives that educate the public about thoughtful use of social media. Such campaigns could be made available in hospitals and clinics, community and senior centers, and other settings where patients or people who use social media congregate.

Social media platforms will evolve as culture, market conditions, and laws change, but platforms are unlikely to go away, so the greatest good will come from approaching social media proactively. Because children are exposed to social media from an early age, social media awareness campaigns have an important role in middle school, secondary school, and university curricula. Age-appropriate information about how social media platforms work, options for sharing personal information, and what to do when things go wrong would prepare young people to become conscientious, meaningfully engaged participants in their health care as adults.

Strong laws that incentivize development of user-friendly platforms with clearly stated data collection practices, use, and sharing policies will play a key role in promoting accountability among social media operators. A ruling by the European Court of Justice in 2014 afforded European citizens the "right to be forgotten." The ruling does not require information to be deleted but requires removal of links from search results for a person. It created differences in international privacy rights, with far-reaching effects on companies such as Google and Facebook, which must treat users in Europe differently and comply with "delinking" requests.[28] In the United States, tort law gives consumers strong protection against incorrect data collected and shared (like wrong credit information) but not against sharing of factually correct information.[29] Legal protection against data collection of individuals in the United States is mainly directed at the federal government and not at companies or individuals. A comprehensive privacy protection system for the United States would include a "Right to be Forgotten" as well as regulation and oversight of data collection,

analysis, and sharing practices. Social media companies, who use security practices to shield themselves from the exposure of their privacy violating practices, are vigorously fighting these initiatives.[30]

Health care is rapidly approaching a critical juncture: though people recognize that they can learn valuable information about maintaining their health and gain support for doing so through the use of social media, health care is in danger of patient rejection of these potential benefits in favor of achieving security of personal information. When social media platforms share information in ways users do not intend as a fundamental part of operations—as opposed to the more common practice of inducing users to agree to it through poorly designed interfaces, complex and confusing language, and privacy setting options that permit only various forms of sharing—users have little choice but to opt out of social media use entirely.

Users of social media find themselves at a fork in the road: Leave social media or remain engaged? But perhaps there is a third option. Perhaps the path forward for the handling of private information in social media mirrors the way researchers are coming to approach the handling of genomic information: "The only path forward is to empower patients to choose the level of privacy they are comfortable with and then attempt to persuade them, one at a time, to make choices that will allow research to go forward."[31] With the passage of legislation prohibiting deceptive practices and the establishment of patient/consumer education campaigns that teach social media users to effectively assess the risks and benefits of social media use, patients will be in a position to use social media for their benefit, rather than primarily for the gain of profit-focused platforms.

Multiple Choice Questions

1. What actions by social media platforms have created the potential for disclosure of health information that users expected would be private?
   a. Sharing of medical records with social media platforms and publication of identifiable social media content in peer-reviewed journals.
   b. Sharing of medical records with social media platforms and sharing of information posted in private groups.
   c. Sharing of information posted in private groups and publication of relationships between users.
   d. Publication of relationships between users and publication of identifiable social media content in peer-reviewed journals.

   Correct Answer: The correct answer is option b, sharing of medical records with social media platforms and sharing of information posted in private groups. Publication of identifiable social media content in peer-reviewed journals requires completion of an informed consent process, so users would not expect their information to remain private. Publication of relationships between users often occurs during use of social media, so users would not expect relationships to remain private.

2. What actions are needed to protect social media users from disclosure of content intended to remain private?
   a. Use of social media platforms based in Europe and greater availability of user education about social media.
   b. Payment of premium user fees and greater availability of user education about social media.
   c. Regulations that give users specific rights related to privacy (e.g., a "right to be forgotten") and greater availability of user education about social media.
   d. Use of social media platforms based in Europe and regulations that give users specific rights related to privacy.

   Correct Answer: The correct answer is option c, regulations that give users specific rights related to privacy and greater availability of user education about social media. Use of social media platforms based in Europe may confer privacy rights on people from that country, but would not necessarily confer rights on others. Payment of premium fees may provide additional services, but the premium may not include services related to privacy.

Protection of Human and Animal Subjects

No human subjects were involved in the creation of this work, so no approval by an Institutional Review Board was required.

Conflict of Interest

None declared.

References

1 Sarasohn-Kahn J. The Wisdom of Patients: Health Care Meets Online Social Media; 2008. Available at: https://www.chcf.org/wp-content/uploads/2017/12/PDF-HealthCareSocialMedia.pdf. Accessed July 29, 2018
2 Knight Foundation. Disinformation, 'Fake News' and Influence Campaigns on Twitter. Available at: https://www.knightfoundation.org/reports/disinformation-fake-news-and-influence-campaigns-on-twitter. Accessed October 19, 2018
3 Kosinski M, Stillwell D, Graepel T. Private traits and attributes are predictable from digital records of human behavior. Proc Natl Acad Sci U S A 2013;110(15):5802–5805
4 Timberg C, Dwoskin E, Zapotosky M, Barrett D. Facebook's disclosures under scrutiny as federal agencies join probe of tech giant's role in sharing data with Cambridge Analytica. Washington Post; 2018. Available at: https://www.washingtonpost.com/technology/2018/07/02/federal-investigators-broaden-focus-facebooks-role-sharing-data-with-cambridge-analytica-examining-statements-tech-giant/?utm_term=.c7dd0c93d5d2. Accessed October 23, 2018
5 Statista. Global social network penetration rate as of January 2018, by region; 2018. Available at: https://www.statista.com/statistics/269615/social-network-penetration-by-region/. Accessed July 29, 2018
6 DeChoudhury M, Kumar M, Weber I. Computational approaches toward integrating quantified self-sensing and social media. CSCW Conference on Computer-Supported Cooperative Work; 2017:1334–1349
7 Frost JH, Massagli MP. Social uses of personal health information within PatientsLikeMe, an online patient community: what can happen when patients have access to one another's data. J Med Internet Res 2008;10(03):e15

8 Pecora V. The culture of surveillance. Qual Sociol 2002;25(03): 345–358
9 Lin WY, Zhang X, Song H, Omori K. Health information seeking in the Web 2.0 age: trust in social media, uncertainty reduction, and self-disclosure. Comput Human Behav 2016;56:289–294
10 Kisekka V, Giboney JS. The effectiveness of health care information technologies: evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. J Med Internet Res 2018; 20(04):e107
11 Berry N, Lobban F, Belousov M, Emsley R, Nenadic G, Bucci S. #WhyWeTweetMH: understanding why people use Twitter to discuss mental health problems. J Med Internet Res 2017;19(04):e107
12 Timberg C, Romm T. Facebook could face record fine, say former FTC officials. Washington Post; 2018. Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/04/08/facebook-could-face-record-fine-say-former-ftc-officials/. Accessed October 23, 2018
13 Federal Trade Commission. Complaint: In the Matter of Facebook, Inc., a Corporation. Federal Trade Commission; 2011. Available at: https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf. Accessed October 23, 2018
14 Richards SE. Facebook's health groups offer a lifeline, but privacy concerns linger. Huffington Post; 2018. Available at: https://www.huffingtonpost.com/entry/facebook-health-groups-lifeline-privacy_us_5b058032e4b07c4ea104098b. Accessed September 19, 2018
15 Madrigal AC. When you're not just the product on Facebook, but the manager. The Atlantic; 2018. Available at: https://www.theatlantic.com/technology/archive/2018/05/when-youre-not-just-the-product-on-facebook-but-the-manager/560864/. Accessed September 19, 2018
16 Farr C. Facebook sent a doctor on a secret mission to ask hospitals to share patient data. CNBC; 2018. Available at: https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html. Accessed April 5, 2018
17 Quinn P. Crisis communication in public health emergencies: the limits of 'legal control' and the risks for harmful outcomes in a digital age. Life Sci Soc Policy 2018;14(01):4
18 Fazzini K, Farr C. Facebook recently closed a loophole that allowed third parties to discover the names of people in private, 'closed' Facebook groups. CNBC; 2018. Available at: https://www.cnbc.com/2018/07/11/facebook-private-groups-breast-cancer-privacy-loophole.html. Accessed October 23, 2018
19 Matsakis L. How a Facebook group for sexual assault survivors became a tool for harassment. Wired; 2018. Available at: https://www.wired.com/story/how-a-metoo-facebook-group-became-harassment-tool/. Accessed July 19, 2018
20 Ferguson C. Predatory behavior runs rampant in Facebook's addiction support groups. The Verge; 2018. Available at: https://www.theverge.com/2018/5/21/17370066/facebook-addiction-support-groups-rehab-patient-brokering. Accessed October 23, 2018
21 Dance GJX, Confessore N, LaForgia M. Facebook gave device makers deep access to data on users and friends. New York Times; 2018. Available at: https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html. Accessed July 29, 2018
22 Reyes I, Wijesekera P, Reardon J, et al. "Won't somebody think of the children?" examining COPPA compliance at scale Proc Privacy Enhancing Technologies 2018;3:63–83
23 Cho H, Filippova A. Networked privacy management in Facebook: a mixed-methods and multinational study. Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work; 2016:503–514
24 Das S, Kramer A. Self-censorship on Facebook. Proceedings of the 7th International AAAI Conference on Weblogs Social Media; 2013:120–127
25 Brown J, Kotz D, Michie S, Stapleton J, Walmsley M, West R. How effective and cost-effective was the national mass media smoking cessation campaign 'Stoptober'? Drug Alcohol Depend 2014;135 (100):52–58
26 Vallone DM, Duke JC, Cullen J, McCausland KL, Allen JA. Evaluation of EX: a national mass media smoking cessation campaign. Am J Public Health 2011;101(02):302–309
27 Wakefield MA, Loken B, Hornik RC. Use of mass media campaigns to change health behaviour. Lancet 2010;376(9748):1261–1271
28 Newman AL. What the "right to be forgotten" means for privacy in a digital age. Science 2015;347(6221):507–508
29 Bernard TS. An $18 million lesson in handling credit report errors. New York Times; 2013. Available at: https://www.nytimes.com/2013/08/03/your-money/credit-scores/credit-bureaus-willing-to-tolerate-errors-experts-say.html. Accessed September 19, 2018
30 Lomas N. Facebook is weaponizing security to erode privacy. TechCrunch; 2018. Available at: https://techcrunch.com/2018/09/29/facebook-is-weaponizing-security-to-erode-privacy/. Accessed October 23, 2018
31 Olson MV. Precision medicine at the crossroads. Hum Genomics 2017;11(01):23