Ethical Issues in Social Media Research for Public Health

Social media (SM) offer huge potential for public health research, serving as a vehicle for surveillance, delivery of health interventions, recruitment to trials, collection of data, and dissemination. However, the networked nature of the data means they are riddled with ethical challenges, and no clear consensus has emerged as to the ethical handling of such data.

This article outlines the key ethical concerns for public health researchers using SM and discusses how these concerns might best be addressed. Key issues discussed include privacy; anonymity and confidentiality; authenticity; the rapidly changing SM environment; informed consent; recruitment, voluntary participation, and sampling; minimizing harm; and data security and management.

Despite the obvious need, producing a set of prescriptive guidelines for researchers using SM is difficult because the field is evolving quickly. What is clear, however, is that the ethical issues connected to SM-related public health research are also growing. Most importantly, public health researchers must work within the ethical principles set out by the Declaration of Helsinki that protect individual users first and foremost. (*Am J Public Health.* 2018;108:343–348. doi:10.2105/AJPH.2017.304249)

Ruth F. Hunter, PhD, Aisling Gough, PhD, Niamh O'Kane, BSc, Gary McKeown, PhD, Aine Fitzpatrick, MSc, Tom Walker, PhD, Michelle McKinley, PhD, Mandy Lee, PhD, and Frank Kee, MD

Social media (SM) are a rapidly evolving set of technologies primarily encompassing a group of social networking sites, such as Facebook and Twitter, that enable efficient, free global communication within a social network. For many people, SM are reshaping their social world, rewriting the rules of social engagement and sociability, and the impact that this has on human behaviors makes it an important avenue for research.[1] SM use has grown nearly 10-fold in the past decade,[2] providing public health researchers with a range of new opportunities for large-scale engagement with the public. SM offer a platform for delivering dynamic, flexible, and interactive content; tailoring messages that express different sentiments; identifying audiences; and providing real-time updates on users' perspectives, and they serve as a vehicle for surveillance, health interventions, recruitment and collection of trial data, and dissemination of results[3,4] at little cost. It is important to acknowledge that each of these uses has different ethical issues.

The networked nature of SM data (i.e., relational data contained in social profiles) is distinct from that of data in traditional variable-based research; data points are not simply collected from individuals and aggregated to provide population estimates; rather, they are composed of interactions between multiple participants, usually on platforms owned by a third party. They are thus ill suited to standard consent models based on assumptions of individual sovereignty over personal data. To date, ethical handling of SM data in research has been controversial, and no clear consensus has emerged. This has resulted in different institutions and institutional review boards (IRBs) putting forward different guidance and recommendations, leaving them to learn through trial and error. Current legislation on data protection and informed consent lags behind the potential of these new technologies, and the ethical principles remain relatively underdiscussed. Moreover, emerging trends in these new technologies, for example, live streaming, make it impossible to predict all the new legal and ethical issues that public health researchers will face.

Public health research must adapt its traditional approaches, and quickly, to ensure that it complies with the highest possible ethical standards to protect the privacy of SM users. The ethical issues identified are relevant in all research contexts, but the fact that every digital interaction can become a unit of data makes these issues far more complex and not always within the researcher's control, nor is it within the control of individual persons to give consent. The rapid evolution of SM technologies means that any ethical guidance for researchers today may have a limited shelf life. Such a rapidly evolving world connotes the Red Queen hypothesis (i.e., "it takes all the running you can, to stay in the same place"). Thus, the aim of this article is not to enshrine inflexible prescriptions on what should or should not be done in every situation, but rather (1) to draw attention to the nature of the ethical considerations relating to SM and (2) to suggest approaches that public health researchers might usefully employ when addressing these ethical challenges.

ABOUT THE AUTHORS

Ruth F. Hunter, Aisling Gough, Niamh O'Kane, Michelle McKinley, and Frank Kee are with the United Kingdom Clinical Research Collaboration Centre of Excellence for Public Health/Centre for Public Health, Queen's University Belfast, Belfast. Gary McKeown and Aine Fitzpatrick are with the School of Psychology, Queen's University Belfast. Tom Walker is with the School of History, Anthropology, Philosophy and Politics, Queen's University Belfast. Mandy Lee is with the Centre for Health Policy and Management School of Medicine, Trinity College Dublin, Dublin, Ireland.

Correspondence should be sent to Ruth F. Hunter, PhD, UKCRC Centre of Excellence for Public Health/Centre for Public Health, Queen's University Belfast, Institute of Clinical Science B, Royal Victoria Hospital, Grosvenor Road, Belfast BT12 6BJ, United Kingdom (e-mail: ruth.hunter@qub.ac.uk). Reprints can be ordered at http://www.ajph.org by clicking the "Reprints" link.

This article was accepted November 9, 2017.

doi: 10.2105/AJPH.2017.304249

OVERARCHING ISSUES

Broadly speaking, the overarching issues pertaining to SM-related public health research are (1) privacy, (2) anonymity and confidentiality, (3) authenticity, and (4) the rapidly changing global environment.

Privacy

Data privacy, defined as "freedom from unauthorized intrusion,"[5(p53)] concerns issues related to privacy options and user controls on SM platforms, as well as the different terms of service provided by each SM platform. Interactions on SM are generally, but not universally, taken to fall somewhere on a private–public spectrum.[6] Others have contended that framing privacy around a public–private dichotomy is unhelpful because the concepts are context and culturally specific and platforms such as Facebook have purposefully worked to erode the concept of privacy by claiming that users want to share all their personal information.[7] However, SM communications and personal profile data leave a permanent online trace, and different users have different privacy expectations, enshrined in generational, social, and cultural norms.[2]

The level of privacy attached to data is dependent on the SM platform and the privacy settings chosen by individual users or platform default settings, which change regularly. One can only properly grasp how to maximize privacy by knowing precisely what the default settings imply and what the users have signed up for. Most SM platforms offer the option to amend privacy settings to control access to profiles and personal information, and users can take specific steps to control the flow of information to different people within their networks, for example, by removing tags from photographs. However, these privacy settings are not particularly user friendly.[8]

Further privacy issues emerge with regard to SM platform terms and conditions, whereby users often register and agree without being fully aware of what they are agreeing to, particularly regarding their personal data.[9] SM companies often make their terms and conditions impossible for even the most conscientious user to comprehend. For example, within Facebook's byzantine policies, including a 14 000-word terms of service, the company has made repeated, often confusing, changes to its privacy policies.[10] A photograph posted on Twitter remains the intellectual property of the user, but Twitter's terms give the company "a worldwide, nonexclusive, royalty-free license (with the right to sublicense)" (File A, available as a supplement to the online version of this article at http://www.ajph.org). The company claims the right "to use, modify or transmit your photograph in any way." In essence, although these platforms claim that you own your content, the corporations involved can use the data however and whenever they want.

Anonymity and Confidentiality

How to deidentify participation in an increasingly networked, pervasive, and ultimately searchable "dataverse" presents a huge challenge to public health researchers—anonymity is ethically crucial. However, because of the traceability of online SM content, anonymity is not always possible, and there have been intense debates on the maintenance and protection of participants' anonymity in SM research (File A).

Although researchers can remove identifying information (e.g., names) from data as per standard IRB practice, other data types that may not appear to identify participants can be vulnerable to disclosure because of the ease of access to and breadth of coverage of online search engines.[11] Although it has been standard practice for IRBs to deal with how individuals may become uniquely identifiable through combinations of attribute variables, and they have guidelines on how to advise researchers proposing such data collection (e.g., reducing demographic variables in survey questionnaires), such procedures are rendered ineffective by the nature of SM data when people's relational links are reliably predictive of their personal attributes.[12] Also, others have demonstrated that anonymization may not be sufficient to protect privacy when dealing with social networks.[13]

The networked nature of the data suggests that these are social profiles rather than individual profiles. SM data such as shared photographs, videos, and identified friendship networks bring their own unique anonymization challenges because of their relational nature. For instance, non–research participants may be tagged in research participants' photographs or videos without their explicit consent. What users say about themselves can also have (unintentional) implications for others—for example, if users state that they have a particular inherited condition. So even if researchers have gained consent to use the primary participant's data, ethical problems will still remain.

Authenticity

Conversely, given the prevalence of anonymous and fake user accounts on SM platforms,[14] ensuring the authenticity of participants' identity can be problematic and affect the validity of SM data and the need for transparency in gaining informed consent. Automated bots are an increasing issue, particularly on Twitter, where they can spam and retweet certain hashtags in an attempt to increase reach and digital footprint.[15,16] Similarly, "astroturfing," in which individuals are employed to adopt false identities and establish a false sense of group consensus, may complicate matters further.

A suite of authentic user detection tools can help combat automated bots.[17] However, astroturfing by state-sponsored actors acting en masse is a harder problem to resolve, especially without an in-depth knowledge of the individuals' online histories—and although making past comments available to online community members is 1 solution, it brings with it other ethical problems: ensuring that researchers collect only data relevant to their specified research purpose and maintaining an individual's right to privacy. When public health researchers study topics that may be seen as politically sensitive by public agencies or corporate interests, the problem of unauthenticated SM users and the solutions proposed to mitigate this problem require proper deliberation.

Rapidly Changing Global Environment

SM are rapidly changing in terms of how people engage with the various platforms, the social and cultural norms that govern their usage, the development of new platforms and the terms and

conditions of their use, platform functionalities, governance, regulations, and legislation. Such factors are situated in a global environment, with no physical borders between countries to dictate which legislation and government rules and regulations should be followed. Researchers therefore need to be cognizant of international laws and expectations.

Furthermore, SM do not operate in a vacuum but are part of the wider media landscape, involving interactions with those of various vested interests. This means that in addition to the traditional research community stakeholders (participants, patients, public, researchers, funders, and journal publishers), a number of other stakeholders are potentially in play—including friends, followers, corporate owners of SM platforms, other commercial interests (those using SM for marketing and promotion purposes), and third-party advocates (such as legal and cybersecurity experts).

Because the law is relatively slow in keeping up with technical developments, the current focus is on self-governance. Researchers must nevertheless consider extant laws in relation to handling SM data. In Europe, the European Union General Data Protection Regulation will change the legal landscape as of May 2018, placing an onus on researchers to provide a clear account of and justification for the good that their research can offer. Part of the General Data Protection Regulation is the right of individuals to request that their data be removed from the dataset. This has important consequences for SM research because online content can be copied and shared rapidly, and researchers are ill equipped to handle deletion requests and rarely check for deleted accounts longitudinally (http://bit.ly/NdpeIu).

RESEARCH IMPLICATIONS

In this section, we discuss key ethical issues to consider throughout the research process (File B, available as a supplement to the online version of this article at http://www.ajph.org). Ethical considerations depend on a range of factors, including the purpose for which SM are being used (e.g., surveillance, intervention, recruitment, dissemination); the public health behavior or condition under investigation; the target population; the role of participants and their networked community; the role of the public health researcher; the SM platform or platforms; and data management. It is beyond the scope of this article to discuss the intricacies of each platform in detail, and researchers should carefully refer to the terms and conditions of each platform because they vary substantially.

Informed Consent

When and how researchers should seek informed consent in an environment that promotes socially mediated and co-constructed texts or that fosters a sense of privacy in the crowd is a significant challenge. This is especially so when consent to taking part in public health research in such environments is inextricably intertwined with how and to what extent users themselves (and their friends and families) might have consented (or not) to sharing their information on SM platforms in the first place.

Relying on implied consent is problematic and should never be the default position in public health research.[18] SM users who knowingly interact publicly on SM sites may not necessarily expect their personal data to be used for research purposes; without changing their privacy settings to reflect this, consent for usage and collection of data are usually implied via the platform's terms of service. However, people are generally uncomfortable with data being used in different contexts from what they originally intended or with being "watched" (http://bit.ly/2EcKo4R).

The lack of clarity around data ownership raises the issue of gatekeeper permission from the SM platform as well as consent from the participant. For example, Facebook's Statement of Rights and Responsibilities now states that, when collecting users' personal data, one must obtain consent, make it clear who is collecting the information, and declare how the data will be used. This change in Facebook's data use policy to explicitly include research was on account of the significant criticism (File A) it received regarding the covert "emotional contagion" study Facebook conducted in 2012 that involved approximately 700 000 of its users, from whom no research consent was obtained, to whom no study information was provided, and who were unable to withdraw from the study. This is a prominent example of how the risks associated with SM health research contrast sharply with those posed in real-world "public crowd" scenarios in standard public health studies, in which the possibility of manipulating individual participants is vastly reduced compared with the personalized nature of SM interactions.[19]

The process by which consent is sought and given in an SM environment also warrants special attention. "Behavioral lock-in" modes of consent, such as "click wrap," that involve users having to actively provide a manifestation of consent by clicking "I agree,"[20] are deemed insufficient by some.[21] Such methods presuppose that users will read the terms before clicking "Yes" to facilitate quick access to services and understand the often lengthy terms and conditions of their service contract with the SM platform—contrary to standard research ethics guidelines about ensuring the comprehension of study information and a standard reflection period between research invitation and consent in traditional health research, ranging from at least 24 hours to as much as 7 days.

Indeed, the fact that the business models of SM platforms are predicated on exploiting user content for profit means that one can no longer apply the assumption that having gatekeeper permission for one's study from the owner of the data platform is any guarantee of robust research governance in the way it has been traditionally understood by the research ethics community. This is especially so when such consent is not based on equal power parity between the individual user and the service provider, and users have few alternatives to participation in such online platforms (e.g., SM accounts being used as a credentialing mechanism). In such contexts, participation is not voluntary but is coerced or, at best, induced.

Accessing user content for public health research from data that are generated in this way by SM platform owners, when informed consent has manifestly not taken place according to the ways it has been understood under the Declaration of Helsinki regarding the right to make informed decisions, raises issues

about research practice that cannot simply be trumped by the public interest argument. The principle of voluntary participation must remain a cornerstone of public health research in the SM era.

More positively alternative methods of obtaining dynamic or meaningful consent have been proposed for SM research,[18,22–24] and an overview of innovative approaches to improving and expanding the informed consent process for researchers and participants in Internet-based trials has been provided by Grady et al.[25] (File B).

Recruitment and Sampling

Using SM as a method for identifying and contacting potential research participants is attractive for public health research because of their wide reach. Two core issues to consider are (1) compliance with the platforms' terms of use and (2) recruitment via the networks of others (e.g., friends, followers), in which researchers seek consent from current or potential participants before soliciting participation from their online network. Researchers are referred to a set of resources developed to help researchers and IRBs navigate through ethical issues specifically for using SM as a recruitment tool.[26]

Minimal verifiable key demographic indicators (e.g., age, race, and gender) can be a major issue when using SM for recruitment and sampling, presenting difficulties in identifying minors and other vulnerable populations and limiting both the inferences that can be drawn and the ability to identify specific populations. Demographic (and other) data are available at the individuals' behest (through their chosen settings) and the SM platform.

Unique to evolving SM technologies are techniques such as facial recognition and machine learning that can infer users' gender, age, race, and location by means of the platform's metadata (see http://bit.ly/2AmCvvW for a review). Demographic data can be inferred from Twitter with reasonable accuracy (60%–90%), which poses concerns for SM users' voluntary participation when their personal information could be given away without their knowledge. The usual modus operandi for IRBs to protect participants' identities has centered on delinking or reducing the amount of personally identifiable information collected by the researcher (e.g., storing personal identifiers away from collected data or restricting the number of demographic variables asked in a survey), but such mechanisms are no longer effective when such demographic data can be predicted via other disclosed data.

Another standard means of protecting participants' identities in traditional variable-based research is to present only aggregate data. However, aggregating data from a group of individuals with a particular sociodemographic characteristic on the basis of the number or nature of the connections that they share actually increases the threat to anonymity. This fact might not be appreciated by most SM users and IRBs.

Furthermore, sampling methods (e.g., tweets to complete a survey) can present issues such as oversampling, because sent and shared messages are quickly beyond researchers' control. Researchers cannot control who sees a shared message, nor can they ensure the accuracy of accompanying information. Promoted messages can help targeting to some extent, but again researchers are beholden to unknown platform algorithms and the level and accuracy of the data provided by the individual. Most SM platforms are now also advertising channels, and individuals are "served" information on the basis of not only their demographic profiles (which they have provided), but also their interests, online behaviors, and prior interactions (which they may not be aware can also be targeted).

Minimizing Harm

Vigilance is required when conducting SM research on sensitive topics that might permit the identification of participants, resulting in stigmatization; the dissemination of findings that could harm an individual or social group; challenges to an individual's values or beliefs; and instances of bullying and abuse. Such research risks inducing or exacerbating emotional distress.[27] Clear distress protocols must therefore be in place from the outset, detailing how such instances will be handled.

This has particular implications for research involving minors and other vulnerable populations. In addition to ensuring that research adheres to specific legislation such as the Children's Online Privacy Protection Rule (https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule) and the Council of Europe's (https://rm.coe.int/168066cff8) recommendations, potential means to minimize harm would be to work with well-established organizations for children and young people that already have a good track record of being involved in ethical online research involving minors. Such ethical practices usually include having robust internal governance structures that are participant led, with young people and members of vulnerable populations involved in well-supported participatory governance processes of reviewing and sanctioning research applications that seek access to their user data.

Similarly, researchers' well-being should be considered when they are being exposed to explicit content, such as extreme or degrading pornographic images; content depicting abusive, violent, or threatening behavior; or content that promotes or condones offensive beliefs (e.g., racism, sexism, and extremism). Appropriate debriefing channels should be put in place to protect researchers' well-being, particularly when dealing with such sensitive issues.

The identity and role of the public health researcher must also be considered. These roles may vary: recruiting participants to trials, delivering interventions and messages, supporting participants, gaining feedback, crowdsourcing, and observing and collecting data. These roles may be carried out silently, via a page or profile or even through fake identities and avatars.[28] Each of these roles comes with its own ethical issues; for example, the perception that researchers are lurking may damage public perception and trust in ways that set back research progress.[29] In every case, though, researchers should minimize the possibility of sanction by acknowledging and following their institution's or their profession's SM guidelines.[15,30] If direct contact with individuals is to occur via SM channels, researchers must decide whether they are to separate their

professional and personal identities or to merge them; they must also remember that even if contact is private, information being exchanged is not always secure and protected.[15] A clear description of the researcher's role, including limitations, should be agreed on at the beginning of a project to ensure consistency and authenticity.

An additional complication in some types of research is the ethical problem of algorithmic timelines and social advertising—that is, the often unequal information to which individuals on SM are exposed.[28] The algorithms controlled by the SM platform choose the information users are exposed to, contingent on machine learning techniques to manipulate their online behavior. Therefore, the SM platform determines what users see, and this process is opaque to researchers.[31] Public health messages disseminated through SM, therefore, may not reach the intended audiences, which has particular issues for minors and other vulnerable populations and poses challenges to both reach and equity.

Data Security and Management

Standard data management issues relating to storage, sharing, security, ownership, and dissemination must be considered. The ethical issues that arise will depend on the source (e.g., streaming, search API, accessing Firehose) and type of data being collected (e.g., sociodemographic information, text, photographs, videos, relationships, geolocation, beliefs, and opinions).

SM data require a high level of security. Security protocols are continually under development, creating standardized tools for ensuring that access to all data are restricted and the data are encrypted. Data curation and analysis carried out on the Internet should be conducted outside the SM platform, and SM data should not be linked to other online information. Data collected on SM are dependent on the security of the platform itself and may be at threat from hackers; this risk is beyond the researchers' control. External survey Web sites may be used to collect public health information, but all data should be stored in anonymized form behind a secure firewall within the research institution.[32]

There are data analysis issues inherent in and specific to SM research. Readers are referred to a number of studies that have discussed constraints and potential solutions.[33–37] Most important, however, the networked (i.e., relational) nature of the data violates the independent data assumptions of most standard statistical analysis techniques, so methods more suited to nonindependent data must be considered.

Finally, how to determine whether a participant has formally withdrawn from a study is difficult. For example, if a user removes data from the SM site (i.e., deletes posts), this does not remove the data from the research database.

A WAY FORWARD

We envisage this article serving as a roadmap to inform and educate both research and SM communities. Opportunities exist to develop resources with an evolving format, such as a wiki page for SM researchers, including a set of training resources for corporate owners of SM platforms, ethics committees, researchers, practitioners, and journal publishers. Indeed, we are starting to see the development of such resources and tools for broader digital technologies,[28,38,39] but there is still scope for further developments. These resources should provide an opportunity for the public health research community to work with other stakeholders rather than in an echo chamber of other like-minded researchers.

Ethical issues connected to SM-related public health research are growing, requiring public health researchers, for now, to view each project on a case-by-case basis and researchers to share their learning as they navigate this new and evolving landscape. Finally, public health researchers must recognize the self-serving interest of SM corporations and work within ethical principles that protect individual users, who are often powerless and uninformed in the labyrinthian SM environment. AJPH

CONTRIBUTORS

R. F. Hunter, A. Gough, G. McKeown, and F. Kee had the original idea for the article. R. F. Hunter drafted the article. All authors attended the consensus workshop on ethical issues in SM-related research in public health, made an intellectual contribution to the draft of the article, and read and approved the final article.

ACKNOWLEDGMENTS

Funding was provided by the Medical Research Council Public Health Intervention Development Scheme. R. F. H. is funded by a Career Development Fellowship from the National Institutes of Health Research and acknowledges funding from the HSC Research and Development Office, Northern Ireland.

We acknowledge the significant contribution made by the members of the Ethics of Social Media Research for Public Health Group, including Laurence Brooks, De Montfort University, Leicester, United Kingdom; Chris James Carter, University of Nottingham, Nottingham, United Kingdom; Nathan Critchlow, University of Stirling, Stirling, United Kingdom; Tristan Henderson, University of St. Andrews, St. Andrews, United Kingdom; Shona Hilton, University of Glasgow, Glasgow, United Kingdom; Luke Hutton, Open University, Milton Keynes, United Kingdom; Marina Jirotka and Helena Webb, University of Oxford, Oxford, United Kingdom; Aileen McGloin, SafeFood, Dublin, Ireland; Dhiraj Murthy, University of Texas at Austin; and Louise O'Hagan, Lindsay Prior, and Paula Tighe, Queen's University Belfast, Belfast, United Kingdom.

HUMAN PARTICIPANT PROTECTION

No human participants were involved in this study and therefore ethical approval was not required.

REFERENCES

1. Qualman E. *Socialnomics: How Social Media Transforms the Way We Live and Do Business*. 2nd ed. New York, NY: Wiley; 2012.

2. Perrin A. Social networking usage: 2005-2015. Available at: http://www.pewinternet.org/2015/10/08/2015/Social-Networking-Usage-2005-2015. Accessed April 18, 2017.

3. Eysenbach G. Infodemiology and infoveillance: framework for an emerging set of public health informatics methods to analyze search, communication and publication behavior on the Internet. *J Med Internet Res*. 2009;11(1):e11.

4. Denecke K, Bamidis P, Bond C, et al. Ethical issues of social media usage in healthcare. *Yearb Med Inform*. 2015;10(1):137–147.

5. Vaidya YZJ, Clifton C. *Privacy Preserving Data Mining*. New York, NY: Springer; 2006.

6. Collmann J, Matei SA, eds. *Ethical Reasoning in Big Data: an Exploratory Analysis*. New York, NY: Springer; 2016.

7. Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press; 2009.

8. Knijnenburg BP, Kobsa A, Jin H. Dimensionality of information disclosure behaviour. *Int J Hum Comput Stud*. 2013;71(12):1144–1162.

9. Obar JA, Oeldorf-Hirsch A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Paper presented at: TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy; September 30–October 1, 2016; Arlington, VA.

10. Montgomery KC. Youth and surveillance in the Facebook era: policy interventions and social implications. *Telecomm Policy*. 2015;39(9):771–786.

11. Zimmer M. "But the data is already public": on the ethics of research in Facebook. *Ethics Inf Technol*. 2010;12(4):313–325.

12. 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.

13. Narayanan A, Shmatikov V. De-anonymizing social networks. Paper presented at: 30th IEEE Symposium on Security and Privacy, May 17–20, 2009; Oakland, CA.

14. Boyd DM, Ellison NB. Social network sites: definition, history, and scholarship. *J Comput Mediat Commun*. 2007;13(1): 210–230.

15. Grajales FJ III, Sheps S, Ho K, Novak-Lauscher H, Eysenbach G. Social media: a review and tutorial of applications in medicine and health care. *J Med Internet Res*. 2014;16(2):e13.

16. Murthy D, Powell AB, Tinati R, et al. Automation, algorithms, and politics bots and political influence: a sociotechnical investigation of social network capital. *Int J Commun*. 2016;10:4952–4971.

17. Davis CA, Varol O, Ferrara E, Flammini A, Menczer F. BotOrNot: a system to evaluate social bots. In: Proceedings of the 25th International Conference Companion on World Wide Web. 2016; 273–274.

18. Luger E, Rodden T. Terms of agreement: rethinking consent for pervasive computing. *Interact Comput*. 2013; 25(3):229–241.

19. Kramer AD, Guillory JE, Hancock JT. Experimental evidence of massive-scale emotional contagion through social networks [published correction appears in *Proc Natl Acad Sci USA*. 2014;111(29): 10779]. *Proc Natl Acad Sci U S A*. 2014; 111(24):8788–8790.

20. Kim NS. *Wrap Contracts: Foundations and Ramifications*. New York, NY: Oxford University Press; 2013.

21. Luger E, Rodden T. An informed view on consent for UbiComp. In: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing. 2013; 529–538.

22. Gomer R, Schraefel MC, Gerding E. Consenting agents: semi-autonomous interactions for ubiquitous consent. In: UbiComp'14 Adjunct: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication. 2014; 653–658.

23. Moran S, Luger E, Rodden T. An emerging tool kit for attaining informed consent in UbiComp. In: UbiComp'14 Adjunct: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication. 2014; 635–639.

24. Hutton L, Henderson T. "I didn't sign up for this!": Informed consent in social network research. In: Proceedings of the 9th International AAAI Conference on Web and Social Media (ICWSM). 2015; 178–187.

25. Grady C, Cummings SR, Rowbotham MC, McConnell MV, Ashley EA, Kang G. Informed consent. *N Engl J Med*. 2017; 376(9):856–867.

26. Gelinas L, Pierce R, Winkler S, et al. Using social media as a research recruitment tool: ethical issues and recommendations. *Am J Bioeth*. 2017;17(3): 3–14.

27. Draucker CB, Martsolf DS, Poole C. Developing distress protocols for research on sensitive topics. *Arch Psychiatr Nurs*. 2009;23(5):343–350.

28. Elovici Y, Fire M, Herzberg A, Shulman H. Ethical considerations when employing fake identities in online social networks for research. *Sci Eng Ethics*. 2014; 20(4):1027–1043.

29. Samuel G. "The Danger of Lurking": Different Conceptualizations of "User Awareness" in Social Media Research. *Am J Bioeth*. 2017;17(3):25–26.

30. Markham A, Buchanan E. Ethical decision-making and Internet research: recommendations from the AoIR Ethics Working Committee (version 2.0). Available at: https://aoir.org/reports/ethics2.pdf. Accessed April 26, 2017.

31. Boyd D, Levy K, Marwick A. The networked nature of algorithmic discrimination. In: SP Gangadharan, ed., with V Eubanks, S Barocas. *Data and Discrimination: Collected Essays*. Washington, DC: Open Technology Institute–New America; 2014; 54–57.

32. Bull SS, Breslin LT, Wright EE, Black SR, Levine D, Santelli JS. Case study: an ethics case study of HIV prevention research on Facebook: the Just/Us Study. *J Pediatr Psychol*. 2011;36(10): 1082–1092.

33. Moorhead SA, Hazlett DE, Harrison L, Carroll JK, Irwin A, Hoving C. A new dimension of health care: systematic review of the uses, benefits, and limitations of social media for health communication. *J Med Internet Res*. 2013;15(4):e85.

34. Alshaikh F, Ramzan F, Rawaf S, Majeed A. Social network sites as a mode to collect health data: a systematic review. *J Med Internet Res*. 2014;16(7):e171.

35. Velasco E, Agheneza T, Denecke K, Kirchner G, Eckmanns T. Social media and Internet-based data in global systems for public health surveillance: a systematic review. *Milbank Q*. 2014;92(1):7–33.

36. Hu Y. Health communication research in the digital age: a systematic review. *J Commun Healthc*. 2015;8(4): 260–288.

37. Townsend L, Wallace C. Social media research: a guide to ethics. Available at: http://www.dotrural.ac.uk/socialmediaresearchethics.pdf. Accessed April 18, 2017.

38. British Psychological Society. Ethics guidelines for Internet-mediated research. Available at: https://beta.bps.org.uk/sites/beta.bps.org.uk/files/Policy%20-%20Files/Ethics%20Guidelines%20for%20Internet-mediated%20Research%20%282017%29.pdf. Accessed April 26, 2017.

39. Torous J, Nebeker C. Navigating ethics in the digital age: introducing Connected and Open Research Ethics (CORE), a tool for researchers and institutional review boards. *J Med Internet Res*. 2017;19(2):e38.