Cyberpsychology, Behavior, and Social Networking
Volume 16, Number 9, 2013

DOI: 10.1089/cyber.2012.0334

Ethics of Social Media Research: Common Concerns and Practical Considerations

Megan A. Moreno, MD, MSEd, MPH,[1] Natalie Goniu,[1] Peter S. Moreno, MS, JD,[2] and Douglas Diekema, MD, MPH[3,4]

Abstract

Social media Websites (SMWs) are increasingly popular research tools. These sites provide new opportunities for researchers, but raise new challenges for Institutional Review Boards (IRBs) that review these research protocols. As of yet, there is little-to-no guidance regarding how an IRB should review the studies involving SMWs. The purpose of this article was to review the common risks inherent in social media research and consider how researchers can consider these risks when writing research protocols. We focused this article on three common research approaches: observational research, interactive research, and survey/interview research. Concomitant with these research approaches, we gave particular attention to the issues pertinent to SMW research, including privacy, consent, and confidentiality. After considering these challenges, we outlined key considerations for both researchers and reviewers when creating or reviewing SMW IRB protocols. Our goal in this article was to provide a detailed examination of relevant ethics and regulatory issues for both researchers and those who review their protocols.

Introduction

Social media Websites (SMWs) provide opportunities for user participation in the creation and display of multimedia data. These popular Websites are increasingly emerging as valuable research tools. There are several aspects of SMWs that provided unique advantages to researchers. First, SMWs present innovative opportunities to examine the displayed online behaviors and beliefs in a context that is naturalistic, as it is part of the participants' daily lives. Second, SMWs allow a researcher to reach out and conduct studies within the populations that may be hard to reach in traditional research, such as underserved populations. Finally, in many cases, this research may be feasible and low cost, as it can be conducted from the researcher's office using a SMW.

SMWs present many new opportunities for research, but also raise new challenges for the Institutional Review Boards (IRBs) that review these research protocols. It remains difficult to determine what risks and privacy expectations are unique to the SMW realm, and what challenges can be addressed by modifications of known and understood risks inherent in research. As of yet, there is little-to-no guidance from federal regulations or institutions, and very little existing literature, on how an IRB should review research protocols involving SMWs.[1]

Given these challenges, the purpose of this article was to review the common risks inherent in social media research and discuss whether these risks represent concerns unique to social media, or modifications to our current understanding of research risks generally. We focused this article on three common research approaches: observational research, interactive research, and survey/interview research. Concomitant with these research approaches, we gave particular attention to issues regarding privacy, consent, and confidentiality. After considering these challenges, we conclude this article by providing key considerations for researchers and reviewers when creating or reviewing SMW IRB protocols. Our goal in this article was not to dictate the rules and regulations for IRBs, but rather to open discussion and outline relevant issues for both researchers and those who review their protocols. Throughout this article, we have framed our discussion around four SMWs that are currently popular: Twitter, YouTube, LinkedIn, and Facebook. Studies of these SMWs illustrate both similarities and differences in social media research techniques and concomitant potential IRB concerns.

Twitter is an SMW in which profile owners (i.e., those with exclusive rights to share information from a certain account)

[1]Department of Pediatrics and [2]School of Law, University of Wisconsin-Madison, Madison, Wisconsin.
[3]Treuman Katz Center for Bioethics, Seattle Children's Research Institute, Seattle, Washington.
[4]Department of Pediatrics, University of Washington, Seattle, Washington.

share short textual information—limited to 140 characters, also called microblogs or tweets—with others in an ongoing, continuously updated RSS feed. Twitter studies as of yet have gathered data regarding individual patient experiences in areas such as pain and smoking cessation, as well as population-level data regarding events such as pandemics.[2–4] YouTube is a video-sharing site that allows the account owners to upload videos, and allows any visitor to view videos. Videos may be user-generated or professionally made. Studies to date have included evaluation of health information within the YouTube videos,[5] assessment of YouTube as a medical teaching tool,[6] and use of YouTube to evaluate an individual's behavior or even symptoms.[7] LinkedIn is a social networking site (SNS) that allows profile owners to share employment and personal information with others. This site focuses on user's professional identities. Studies to date include basic analyses of the LinkedIn users, comparing them to the Facebook users.[8]

Currently, the most popular SNS is Facebook, which allows profile owners to create an online profile, including displayed personal information via text, video, surveys, or photographs, to build an online social network by friending profile owners, and to communicate with other profile owners via messaging.[9] Studies to date include evaluation of displayed content by profile owners, including health risk behavior information such as sexual behavior and substance use, mental health, and personality characteristics.[10–15]

Common Regulatory Concerns with Social Media Research

As with all types of research, there are potential risks to participants in studies involving SMWs. We have focused on three specific research approaches that researchers and IRBs may encounter when considering federal and institutional regulations that involve SMWs: observational, interactive, and survey/interview. For each of these, we considered relevant risks and framed those risks within the context of traditional research as appropriate. Because the issues regarding privacy concerns in observational research may apply to the other two research approaches, we address the observational research first.

Observational research

A key issue in considering observational research using social media is whether the proposed project meets the criteria as human subjects research, and if so, what type of review is needed. A human subject is defined by federal regulations as a living individual about whom an investigator obtains data through interaction with the individual or identifiable private information. If the following conditions are met, access to the SMW is public; information is identifiable, but not private; and information gathering requires no interaction with the person who posted it online, and then presumably the proposed project does not constitute the human subjects research. For example, an observational study of YouTube videos involves publicly posted and available content accessible to any Internet user. In this case, the information is not private, and it does not require any interaction with the subject to access it.

Observational research may also meet the criteria for exemption from the IRB review if the study involves observation of public information regarding individual human subjects. Exempt research includes research involving the observation of public behavior, except when information obtained is (a) recorded in such a manner that subjects can be identified either directly or through the identifiers linked to the subjects, or (b) any disclosure of subjects' responses outside the published research that could reasonably place the subjects at risk of criminal or civic liability, or be damaging to the subjects' financial standing, employability, or reputation. This category of research would likely apply to an investigator observing Websites such as Facebook or LinkedIn, provided that only publicly available profiles were evaluated to make collective observations. It is important to note that this category does not apply to minors if the investigator participates in the activities being observed. Thus, as long as one does not participate by interacting with participants, such as trying to establish connections between profiles via friending, this would seemingly apply to minors' displayed content on SMWs.

Recent changes in the SMW policies and controversies related to particular studies have raised new issues regarding whether observation of the public behavior via SMWs should continue to receive the IRB approval.[16] At one state university, the IRB's review and interpretation of the Facebook Rights and Responsibilities statement led to controversy over whether an SMW-based study could be approved. At the time of this article, this Facebook policy stated "If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it." This debate regarding privacy concerns in observational research, and SMW research generally, involves three major topics: user involvement in privacy protection, Website privacy guidelines, and legal considerations.

User involvement in privacy settings and Website access. Some SMWs allow the users to choose their own privacy settings. On Facebook and LinkedIn, for example, profile owners have the choice to protect their displayed information through profile security settings.[17,18] Profile security settings can be private (i.e., limiting some or all profile information access to online friends approved by the profile owner), or public (i.e., allowing any user access to the profile). Privacy settings can limit access to the profile as a whole, or settings can be customized to limit access to certain profile viewers or to particular sections of the profile. Similar settings are available on Twitter. Thus, participants can choose whether or not their posted content is publicly available, which may in turn affect whether an IRB views the observation of this content as an exempt or otherwise permissible research.

In the past, some IRBs have considered whether or not the Website itself requires a username and password login to determine if the site is of a public or private nature. If a username and password were required, the site was not considered public, and thus the consent could be required to view content. Newer SMWs raise concerns about whether that policy can still guide these decisions, because many SMWs require usernames and passwords for only particular purposes or only under certain circumstances. YouTube, for example, requires a username and password to verify one is over the age of 18 to post videos and view videos of adult content. Anyone may view general YouTube videos, with or

without a username or password. One would therefore not expect that the consent would be required to conduct an observational study of general YouTube videos. Other SMWs such as Facebook require a username and password to ensure that only the profile owner posts information to his or her page, and to provide tailored advertisements to users and data to marketing companies. The availability of the information posted, however, is determined by the profile owner, who can expressly make the information available to the public. Thus, old paradigms of IRB rules related to Internet research may need reconsideration.

Website purpose and privacy statements. A reasonable expectation of privacy for an SMW user is comprised of a combination of the intent of the Website as well as the Website's explicit statement of privacy rules. The most consistency between Website intent and Privacy Policy is that of Twitter, which explicitly stated "our Services are primarily designed to help you share information with the world …… Our default is almost always to make the information you provide public but we generally give you settings to make the information more private if you want. Your public information is broadly and instantly disseminated."

Similarly, YouTube's statement of intent of being a forum of sharing videos publicly is consistent with their Privacy Policy. At the time of this article, this policy stated that one "may control the information that is available to other users and your confirmed friends at any time."

The statement of intent for LinkedIn is "connecting the world's professionals." This statement has consistency with the site's Privacy Policy, which stated "The information you provide to LinkedIn may reveal, or allow others to identify, your nationality, ethnic origin, religion, gender, age, geography, or other aspects of your private life." These synergistic statements present a clear expectation that the responsibility of the content of displayed information and its protection lies with the profile owner.

As we now return to the Facebook Privacy Policy, the described intention of the site was to share information with people. This intent was reflected in the first part of the Privacy Policy, which states "When you publish content or information using the 'everyone' setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)." Further in the Privacy Policy, a statement indicated "Information set to 'everyone' is publicly available information….Such information may, for example, be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third-party search engines and be imported, exported, distributed and redistributed by us and others without privacy limitations." These statements demonstrated clear wording and were directed at the user. Thus, Facebook informed the user that if the profile security settings are publicly available, the profile owners should not have a reasonable expectation of privacy.

Facebook also discussed access to information by third parties through these statements: "We generally limit search engines' access to our site. We may allow them to access information set to the 'everyone' setting (along with your name and profile picture) and your profile information that is visible to everyone." Facebook then explained how this access to information by third parties can be avoided: "You can change the visibility of some of your profile information using the customize section of your privacy settings."

Separate from the Privacy Policy was a Rights-and-Responsibilities hyperlink. This section explained, "If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it." This statement appeared to be directed at a third party, such as a researcher who aimed to collect information from Facebook profiles. Thus, a contradiction exists between the statements in the Privacy Policy compared to the Rights and Responsibilities sections regarding their intended audience as well as their direction.

Legal considerations. Many IRBs seek guidance from court cases involving the invasion of privacy to determine what would constitute a privacy violation in the research context. Under the Fourth Amendment to the U.S. Constitution, individuals are protected from governmental searches when and where they have a reasonable expectation of privacy. This expectation is limited by what society recognizes as reasonable, given the circumstances of the individual at the time of the search. Courts have held, for example, that an individual generally has a reasonable expectation of privacy within his or her own home, but does not have a reasonable expectation of privacy in things the individual knowingly exposes to the public.[19] The right to privacy is similarly recognized in civil cases between nongovernmental parties. A defendant can be liable, for example, when he or she makes public disclosures of private facts about the plaintiff. Courts deciding such cases often apply a reasonable expectation of privacy analysis to the alleged disclosure, typically finding that a fact is private when a reasonable person in the plaintiff's position would expect the fact to be private.

Federal and state courts have examined Facebook's privacy policy and determined that individuals do not have a reasonable expectation of privacy in information they post on their Facebook pages. In Romano v. Steelcase (2010), the plaintiff Romano sued the Steelcase Company for damages, claiming that their actions had caused her permanent injury and suffering. Steelcase sought information from Romano's current and historical Facebook accounts, including deleted pages, to rebut these claims. The court granted Steelcase's request to access the information on these pages, holding that Romano did not have a reasonable expectation of privacy in information that she published on social networking Websites. The court noted that Facebook privacy policies plainly state that information users' post may be shared with others, and that information sharing is the very nature and purpose of these SNSs, else they would cease to exist. Courts have concluded that a person has no reasonable expectation of privacy in writings that the person posts on a social networking Website and makes available to the public.[20] Another court concluded that users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting.[21] This has become a generally accepted principal of law (92 A.L.R. 5th 15§ 4.5).

Interactive Research

Interactive research takes place when a researcher wishes to assess the SMW content that is not publicly available. To

access this information, the researcher needs to contact the participant for permission to view the content. On Facebook, this interaction may include a friend request. Some have argued that a friend request may lead to a misrepresentation of the researcher's intentions for the relationship. Similarly, on Twitter, access to protected Tweets means that the researcher must become a follower of that participant, also potentially implying a closeness of relationship. It is important to recognize that the terms "friending" and "following" have very different meanings for those inhabiting today's social media world. Previous studies have determined that Facebook friending implies a loose-tie relationship, often including associates or acquaintances.[12] Further, the absolute number of Facebook friends is often considered a marker of positive social capital.[12,22] On Twitter, users can be followers of people they have never personally met, such as celebrities and politicians. Thus, both friending and following in and of itself are unlikely to trigger unreasonable expectations for a close or prolonged relationship on the part of participants.

If the researcher conducts a study involving minors, it is likely that including friending or following would constitute interaction and participation in the research venue. In this type of study, it is worth considering the categories of research that include waivers of parental consent. An IRB may approve a consent procedure that does not include parental consent if the project involves no more than minimal risk to the participants; the waiver will not adversely affect the rights and welfare of the subjects; the research could not be practically carried out without the waiver; and the subjects will be provided with additional pertinent information after participation when appropriate.[23]

Survey/Interview Research

Risks regarding consent in the SMW arena

Two potential concerns exist when conducting informed consent online. A first concern is the lack of face-to-face contact with participants. When approaching participants on SMWs, or collecting data from the online representations of participants, there are often situations in which the researcher has no direct face-to-face contact with the participant. Thus, there may be reduced opportunities for the researcher to observe participant reactions to the consent process. Concerns regarding the lack of physical interaction during the consent process are more salient when the study collects information that is potentially illegal or stigmatizing, or when the study participant will be from an at-risk population such as minors or people who are cognitively impaired.

This is a valid concern, but not one that is unique to SMWs. Many research studies employ mailed surveys and consent forms, situations that do not provide opportunities to interact with participants. It is also possible that online recruitment and consent processes may increase the likelihood that a researcher will hear from participants if questions or concerns arise when compared to mailed surveys. Given that people may be more likely to lash out inappropriately or flame online, there is the implication of a heightened sense of security and safety when conversing over the Internet. Hence, this may increase the likelihood that the participant will contact the researcher online with questions arising from an online consent form compared to the participant taking the effort to call to address the concerns about a mailed consent form.

A second concern is how to obtain parental consent. Federal research regulations state that minors under the age of 18 years must have parental consent and minor assent to participate in most research trials, unless the study receives a waiver of parental consent. Obtaining parental consent in a study that involves recruitment through SMWs provides new challenges, as a minor may be able to complete the parental consent process posing online as the parent. Adolescents are typically more Internet savvy than their parents and may find this process quite simple. However, this risk is not unique to SMW research. Minors can and have easily forged their parent's signature using traditional paper consent forms. Although representing a parent's consent online by checking a box may be easier than forging a parent's signature, both methods are possible and easily achieved by a modern adolescent.

Confidentiality: A Key to Any Social Media Research Approach

An important area of concern with SMW research is the protection of confidentiality. Similar to other types of research involving survey or interview data, protection of participant identities is critical. Website research may initially be perceived as lower risk, because participant information can be collected in absence of some Health Insurance Portability and Accountability Act (HIPAA)-protected information such as address or phone number. Online data can present increased risks; studies that publish direct text quotes from an SMW may directly identify participants. Entering a direct quote from an SMW into a Google search engine can lead to a specific Web link, such as a link to that person's LinkedIn profile, and thus identify the participant.

Presenting unique combinations of data that are linked to individuals may also identify participants. These concerns were clearly demonstrated through controversy surrounding the Tastes, Ties, and Time project.[16] In this project, researchers downloaded a large dataset of Facebook information from a single university. The identities of some participants were eventually determined based on the uniqueness of the information presented. The university was identified through the list of college majors represented in the study population. Further, some participants were identified by being a member of an under-represented minority group. This project stirred ongoing controversy regarding confidentiality within Facebook research.[24]

Recommended Considerations

To conclude, SMWs are immensely popular and present new opportunities for research as well as new challenges for IRBs to evaluate these proposals' risks and benefits. In considering risks of SMW research, IRBs should balance consideration of unique risks with those consistent with traditional research methods.

Thus, specific recommendations for researchers and IRBs include the following:

Observational research

- IRBs should consider whether the proposed study meets criteria as the human subject research. For example, an analysis of YouTube videos depicting dental hygiene

practices is a study involving video clips, not human subjects. As another example, a researcher proposes to study how many Facebook pages depict images of families without collecting any profile owner identifiers on the page such as age, sex, or location. In this case, the unit of analysis is the page rather than the profile owner.

- IRBs should give consideration to the risk level and content of the study. For example, a project that evaluates how many times a 12-year-old tweets the word "like" has a low risk level. In contrast, a project that observes an online group discussion of adolescent HIV patients to see which ones report noncompliance with medications has a higher risk level. Increased attention should be devoted to higher-risk studies, concomitant with a higher threshold to grant waiver of the participant consent. IRB proposals that include collection of illegal or stigmatizing information from SMWs, or involve data collection from minor's SMW profiles, should be considered carefully.

Interactive research

- Researchers should present an accurate portrayal of their identity on SMWs, but undue concerns regarding participants' investment in the relationship defined by friending or following is likely unnecessary.

Survey/interview research

- Researchers should provide contact information for questions during the consent process, including contact information online and via SMW that can be monitored and responded to quickly.
- In the future, SMW researchers should consider using SMWs to obtain parental consent for adolescents' participation in research studies, as parents are increasingly becoming the members of the SMW sites such as Facebook.[25]

Overall Recommendations

(a) To protect confidentiality, researchers should understand the risks of and avoid direct text quotes in presenting SMW text quotations from research subjects. Researchers should avoid presenting participants' personal information in the ways that they could be identified within their schools or communities.

(b) One Facebook section, Applicable to Developers/Operators of Applications and Websites, included the following statement at the time of this article: "you will only request data you need to operate your application." This section also instructed outside parties: "you will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data." Researchers should consider applying these principles by only collecting the essential data needed to answer the research question, and presenting those data carefully to avoid participant identification. Researchers should consider listing a privacy policy on their laboratory Webpages, as well as developing a laboratory SMW page that describes what data they use and how they are used. One possible strategy is to develop a Facebook page as a professional identity for the principal investigator or staff, separate from a personal Facebook page. In this way, participants can friend the researcher in a professional rather than personal context.

(c) A little-recognized, but challenging, issue is that each state has its own law regarding informed consent. This includes how the consent should be documented and the age at which consent can be obtained for various health topics. How, or whether, this process applies to SMW is unclear. If the researcher is located in Illinois and conducting a multistate survey of Twitter users, what level of regulation should take precedence? This issue merits further discussion and consideration as researchers move toward more fully harnessing the global research opportunities provided by SMWs.

Acknowledgments

Funding for this project was provided in part by the University of Wisconsin Graduate School. The authors would like to acknowledge the contributions of Lil Larson, Jessica Hirsch, and Monet McGruder to this project.

Author Disclosure Statement

No competing interests are present for any author.

References

1. Moreno MA, Fost NC, Christakis DA. Research ethics in the MySpace era. Pediatrics 2008; 121:157–161.
2. Chew C, Eysenbach G. Pandemics in the age of Twitter: content analysis of Tweets during the 2009 H1N1 outbreak. PLoS One 2010; 5:e14118.
3. Heaivilin N, Gerbert B, Page JE, et al. Public health surveillance of dental pain via Twitter. Journal of Dental Research 2011; 90:1047–1051.
4. Prochaska JJ, Pechmann C, Kim R, et al. Twitter = quitter? An analysis of Twitter quit smoking social networks. Tobacco Control 2012; 21:447–449.
5. Paek HJ, Hove T, Kim M, et al. Mechanisms of child abuse public service announcement effectiveness: roles of emotional response and perceived effectiveness. Health Communications 2011; 26:534–545.
6. Baer W, Schwartz AC. Teaching professionalism in the digital age on the psychiatric consultation-liaison service. Psychosomatics 2011; 52:303–309.
7. Bowen LN, Malaty IA, Rodriguez RL, et al. Did General Douglas MacArthur have Parkinson disease? A video and archival analysis. Neurology 2011; 76:1668–1672.
8. Papacharissi Z. The virtual geographies of social networks: a comparative analysis of Facebook, LinkedIn and ASmallWorld. New Media Society 2009; 11:199–220.
9. Lenhart A, Purcell K, Smith A, et al. (2010) *Social Media and Young Adults.* Washington, DC: Pew Internet and American Life Project.
10. Moreno MA, Parks MR, Zimmerman FJ, et al. Display of health risk behaviors on MySpace by adolescents: prevalence and associations. Archives of Pediatrics and Adolescent Medicine 2009; 163:35–41.
11. Christofides E, Muise A, Desmarais S. Information disclosure and control on Facebook: are they two sides of the same

coin or two different processes? Cyberpsychology and Behavior 2009; 12:341–345.
12. Ellison NB, Steinfield C, Lampe C. The benefits of Facebook "Friends:" social capitol and college students' use of online social network sites. Journal of Computer-Mediated Communication 2007; 12:1143–1168.
13. Lewis K, Kaufman J, Christakis N. The taste for privacy: an analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication 2008; 14:79.
14. Mauri M, Cipresso P, Balgera A, et al. Why is Facebook so successful? Psychophysiological measures describe a core flow state while using Facebook. Cyberpsychology Behaviors Social Network 2012; 14:723–731.
15. Pempek TA, Yermolayeva YA, Calvert SL. College students' social networking experiences on Facebook. Journal of Applied Developmental Psychology 2009; 30:227–238.
16. Lewis K, Kaufman J, Gonzalez M, et al. Tastes, ties, and time: a new social network dataset using Facebook.com. Social Networks 2008; 30:330–342.
17. Baym NK, Boyd D. Socially mediated publicness: an introduction. Journal of Broadcast Electron 2012; 56:320–329.
18. Boyd D, Marwick A. Social privacy in networked publics: teens' attitudes, practices and strategies. A decade in internet time. *Symposium on the Dynamics of the Internet and Society*; 2011.
19. Weeks MR, Convey M, Dickson-Gomez J, et al. Changing drug users' risk environments: peer health advocates as multi-level community change agents. American Journal of Community Psychology 2009; 43:330–344.
20. Geibel S, Luchters S, King'Ola N, et al. Factors associated with self-reported unprotected anal sex among male sex workers in Mombasa, Kenya. Sexually Transmitted Diseases 2008; 35:746–752.
21. Luchters S, Chersich MF, Rinyiru A, et al. Impact of five years of peer-mediated interventions on sexual behavior and sexually transmitted infections among female sex workers in Mombasa, Kenya. BMC Public Health 2008; 8:143.
22. Lin KY, Lu HP. Intention to continue using Facebook fan pages from the perspective of social capital theory. Cyberpsychology and Behavior Social Network 2011; 14: 565–570.
23. Services UDoHaH. (2009) *Code of Federal Regulation*. In: HHS, ed. Vol 45 CFR 46.116.
24. Zimmer M. "But the data is already public": on the ethics of research in Facebook. Ethics and Information Technology 2010; 12:313–325.
25. Tokunaga RS. Following you home from school: a critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior 2010; 26:227–287.

Address correspondence to:
Dr. Megan A. Moreno
Seattle Childrens Research Institute
University of Washington, Department of Pediatrics
M/S CW8-6 PO Box 5371
Seattle, WA 98145-5005

E-mail: megan.moreno@seattlechildrens.org