

# “The Danger of Lurking”: Different Conceptualizations of “User Awareness” in Social Media Research

Gabrielle Samuel, Lancaster University

Using detailed real-life examples, Gelinis and colleagues (2017) have provided a much-needed description of how researchers and U.S. institutional review board (IRB) members should ideally handle issues that emerge when researchers wish to recruit research participants via social media. The authors’ approach is nonexceptionalist, arguing that recruitment should be ethically evaluated in the same way as the more traditional analogue or “offline” recruitment (an approach we have identified in our empirical research as a broad ethical strategy for much social media ethics). Using an empirically driven approach that draws on the views of those for whom the guidelines are intended, my research highlights areas in which these guidelines are lacking.

I draw on a series of interviews with a range of UK research ethics committee (REC) members whom can be viewed, for the premise of Gelinis and colleagues’ article, as analogous to IRB members in the United States. During these interviews REC members’ views, experiences, and decision making were explored with relation to the use of social media for data collection. While Gelinis and colleagues’ guidelines have been purposively narrowly defined for using social media as a recruitment tool rather than for data collection, an analysis of the interview findings suggests they can still add value by highlighting areas in which the guidelines are lacking.

For example, a number of interviewees spoke about the range of issues associated with research exploring social media data from the Dark Web; from “hate” speech; or from otherwise hard-to-reach groups, such as those linked to, or persecuted by, terror organizations (data that may be health related or otherwise). Considerations of these types of data is lacking from the authors’ guidelines, providing little instruction (e.g., in terms of safety and other governance issues) for those wishing to possibly recruit from such data platforms. In addition, other interviewees spoke about the ethical considerations related to scientific validity and contextualization—considerations that, while not unique to social media research, were again missing from Gelinis and colleagues’ discussions. For instance,

researchers need to be aware that when recruiting via social media platforms, it may be difficult to confirm the age of any potential research participant (i.e., evidence that the participant is not a minor), or that their identity is reported truthfully, especially if recruitment is for online rather than face-to-face surveys/interviews.

Our findings also highlight the ambiguity of Gelinis and colleagues’ recommendation that “proposed recruitment does not involve members of a research team ‘lurking’ on social media sites in ways members are unaware of,” as well as the authors’ statement that whether or not a researcher should alert social media users to their presence (i.e., not “lurk”) “depends largely on whether the site is . . . viewed as a public or private space. The more public a social media venue is . . . the less of a reasonable expectation of privacy users of the site have, and the less of an obligation investigators have to proactively disclose their presence” (6). I spend the remainder of the commentary discussing this in more detail in the following.

## RESEARCH ETHICS COMMITTEE INTERVIEWS

All interviewees were in agreement with Gelinis and colleagues’ assertions that social media users may not fully understand or be certain about what can and cannot be publically viewed on social media platforms. Interviewees explained that this was because users often interact with publically available social media platforms in “closed” spaces, giving them a sense of apparent privacy: “[Users] think it’s a lot more private because it’s sort of me and the computer or me and my iPad or whatever it might be. And not fully understanding that actually that’s not really like that. It’s much more open” (interviewee 12). However, interviewees had a range of opinions as to whether any user unawareness about the public nature of social media platforms needed to be considered during REC members’ ethical decision making.

When talking about “public” social platforms, defined here as requiring no user name or password,

Published with license by Taylor and Francis. © Gabrielle Samuel. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Address correspondence to Gabrielle Samuel, Department of Educational Research, Lancaster University, Lancaster, LA1 4YD, United Kingdom. E-mail: [gabbysamuel@googlemail.com](mailto:gabbysamuel@googlemail.com)

some interviewees felt the onus of responsibility “to know it’s public information” was on social media users themselves: “I tend to think that people have a certain responsibility for themselves” (interviewee 10). Using such data was “fair game” and researchers were under no obligation to gain consent for such purposes: “People put data out into the public domain, it’s in the public domain. I mean what do they expect” (interviewee 6). If we analogize this to the social media recruitment recommendations proposed by Gelinias and colleagues, the assumption here is that data are public. As such, there is little expectation for privacy and researchers have little obligation to disclose their presence if drawing on or recruiting from the data.

Other interviewees disagreed. They believed that researchers/REC members must take responsibility to protect social media users who may have less understanding of the platforms they are engaging with and that researchers are always obliged to respect social media users’ (data), even when on a public platform: “There is something questionable about using tweets even if they’re not identifiable . . . it seems to me to echo that point I made about, because it’s a tweet its fair game and I think that’s to be questioned” (interviewee 14). Analogizing to Gelinias and colleagues’ guidelines, the assumption here is that because social media users may be unaware of the public nature of their data, researchers—in an effort to not be seen as “lurking”—have an obligation to respect user privacy by disclosing their presence when using data or recruiting participants.

Differences in interviewees’ perceptions also extended to data usage from more “private” social media spaces, defined here as requiring a username and password, such as chatrooms. For example, most interviewees explained that private chatroom data should be considered ethically in much the same careful way as face-to-face settings: “If it was something you need your own username and password and it was very clearly locked down . . . we would want them to deal with it much more as if they were dealing with specific individuals in a face-to-face setting” (interviewee 11). If we again analogize this to Gelinias and colleagues’ guidelines, these chatrooms constitute a private space and any researcher “entry” into the chatroom

without permission (e.g., from a moderator, or via consent of the platforms users) would be against a researcher’s obligations to disclose his or her presence and would constitute “lurking.” Others took a more liberal view of the definition of “lurking.” For them, choosing not to disclose a researcher’s presence in a chatroom did not always amount to “lurking.” If researchers are “only interested in what they [the users] say, not who they are,” then it was ethically appropriate to “err on the side of being pretty liberal as long as the investigator was simply an observer [of the discourses]” (interviewee 10).

In conclusion, this commentary has highlighted two areas in which Gelinias and colleagues’ recommendations have a lack: through missing discussions, and in the different ways in which REC members interpret their obligations to social media users in terms of when, or if, it is appropriate to use data without permission. In terms of the latter, this suggests researchers/IRB members may also have differences in perceptions about the appropriateness of “lurking” when researchers recruit through social media platforms.

Such issues with social media guidelines are not new (for a discussion see Whiteman, 2012; our research [unpublished]). They represent the difficulties scholars are having with identifying best standards of practice in this new research field. However, it is important that we resolve how social media data are being interpreted by researchers/RECs/IRBs before relevant guidelines can be outlined and reflected in ethically sound research practice. From my perspective, any guidelines preceding such resolve must be explicit in terms of this vagueness so that researchers are aware of the difficulties within the research field and can approach their ethical decision making with this in mind (e.g., on case-by-case bases). ■

## REFERENCES

- Gelinias, L., R. Pierce, S. Winkler, I. G. Cohen, H. F. Lynch, and B. E. Bierer. 2017. Using social media as a research tool: Ethical issues and recommendations. *American Journal of Bioethics* 17 (3):3–14.
- Whiteman, N. 2012. *Undoing ethics: Rethinking practice in online research*. London, UK: Springer.