Practical Suggestions for Legal and Ethical Concerns with Social Environment Sampling Methods

Megan L. Robbins

University of California, Riverside

In press at *Social Psychological and Personality Science*

Megan L. Robbins has been an Assistant Professor in the Department of Psychology at the University of California, Riverside since 2013. She received her doctorate in Psychology from the University of Arizona, and her bachelor's degree from the University of Texas in Austin. Her research focuses on understanding how people's daily social interactions are related to health and well-being.

Megan L. Robbins, PhD
Department of Psychology
University of California, Riverside
900 University Ave.
Riverside, CA 92521
Email: megan.robbins@ucr.edu

Abstract

The capabilities offered to psychology researchers by new technology have catapulted the field toward a deeper understanding of people's social experiences. However, it concurrently increases the need to consider the ethical and legal concerns of capturing information about bystanders. This paper outlines the legal and ethical issues that researchers should consider when conducting social environment sampling research. The goal is to serve as a "quick start guide" to the unique legal and ethical challenges that arise with social environment sampling, and to offer some solutions.

Keywords: EAR, ambulatory assessment, social media

Technology has provided psychology researchers with an exciting and growing set of methodological tools. Instead of solely relying on retrospective accounts and in-lab behavior, researchers are also able to unobtrusively listen to naturally-occurring conversations (e.g., Mehl & Pennebaker, 2003; Robbins, López, Weihs, & Mehl, 2014), visually observe everyday situations (e.g., Brown & Sherman, under review), link physical activity to participants' real-time location (Worringham, Rojek, & Stewart, 2011), and so much more (Ben-Zeev et al., 2016; Mehl & Conner, 2012; Miller, 2012). Because they enable observational data collection on a larger scale than could be achieved by physically observing people in their natural environments (Barker & Wright, 1951), these methods facilitate a more comprehensive understanding of personality and social behavior than was previously possible.

For example, the Electronically Activated Recorder (EAR; Mehl, Pennebaker, Crow, Dabbs, & Price, 2001; Mehl, Robbins, & Deters, 2012) is a small device participants wear on their waistline that records brief audio clips as participants go about their normal days. As a naturalistic observation method, the EAR yields an audio sample of daily life. The EAR has been used in an array of studies, from debunking lay theories about women talking more than men (Mehl, Vazire, Ramírez-Esparza, Slatcher, & Pennebaker, 2007), to uncovering how personality manifests in daily life (Mehl, Gosling, & Pennebaker, 2006), and revealing the frequency of cancer conversations among couples coping with breast cancer (Robbins et al., 2014).

Another social environment sampling method naturalistically observes visual information, yielding a "lifelog" of situations participants encounter. One such device is the Narrative, which periodically captures photos while worn near the participant's chest, typically by necklace or clip (Brown & Sherman, under review). Lifelogging methods have been used to

understand reasons people go from one situation to another (Brown & Sherman, under review), as a retrospective memory aid (Hodges, Berry, & Wood, 2011), and as an observational measure of dietary intake (Sun et al., 2010).

The third major class of social environment sampling methods is electronic communication—via emails, text messages, or social media. A growing body of social psychological and personality research has tapped the seemingly unlimited uses of this readily available data on naturally-occurring social behavior. Studies have spanned a variety of topics, often focusing on antecedents and psychological outcomes of Facebook (Anderson, Fagan, Woodnutt, & Chamorro-Premuzic, 2012) and Twitter use (Zimmer & Proferes, 2014). Researchers have also examined social dynamics within email (Tausczik, Chung, & Pennebaker, 2014) and private messaging communication (Slatcher & Pennebaker, 2006).

Using such technology in psychological research greatly advances understanding of social behavior and environments; however, it concurrently increases the need to consider the ethical and legal concerns of capturing information about bystanders. These legal challenges are unique to methods that sample social environments (hereafter referred to as *social environment sampling*) because other methods of observing daily life collect data only from the consenting participant (e.g., salivettes for cortisol, accelerometer for physical activity, Ecological Momentary Assessment of mood). The goal of this article is to serve as a "quick start guide" to considering the unique legal and ethical challenges that arise with social environment sampling, and to offer some practical suggestions.

It is important to note that the author of this paper is a psychology researcher, not a lawyer. The information presented here reflects the author's first-hand experience navigating

several states' laws that pertain to social environment sampling, as well as second-hand consulting with researchers in various other states, consultation with lawyers at the author's institution, and review of published legal opinions. Legal opinions often differ, and therefore this paper is meant to serve as a starting point for considering legal and ethical implications of social environment sampling in research, and not as a substitute for one's own legal counsel. Further, this article does not intend to resolve all legal and ethical challenges associated with social environment sampling; rather, the purpose is to lay out some relevant considerations and practical solutions that may aid researchers in designing their studies. The considerations discussed here may apply to other countries as well, but for conciseness this paper focuses specifically on U.S. law.

Legal Considerations

One- and All-Party Consent Recording Laws

In the U.S., there are several types of statutes that may apply to social environment sampling. One of the types most relevant to social environment sampling is wiretapping law, initially intended to protect people from their phone calls being intercepted and recorded by anyone not directly involved in the conversation. However, technology has necessitated that these laws expand to regulate the use of the multiple recording functions on smartphones. For example, federal law states that it is illegal to "intercept any wire, oral, or electronic communication" (18 U.S.C.S. § 2511), and each state has their own laws on recording communication between people. In their original form, wiretapping laws addressed audio data, thus audio recordings are more consistently protected by state laws than are video recordings. However, these laws implicitly (sometimes explicitly) extend to video recordings with an audio

track (Reporters Committee for Freedom of the Press, 2012), and laws increasingly address the collection of data via visual-only channels.

An important distinction in the U.S. wiretapping laws is whether they require one- or two-party consent. One-party consent laws dictate that only one person involved in the conversation needs to consent to its recording. On the other hand, two-party consent laws require the consent of all people involved in the conversation to legally record it. For clarity, two-party consent will hereafter be referred to as *all-party consent*. Most states in the U.S. are one-party consent states, but approximately 13 states—California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Oregon, Pennsylvania, and Washington—require all-party consent for at least some types of recording (legal opinions differ on the interpretation of these laws; e.g., Matthiesen, Wickert, & Lehrer, 2016; Reporters Committee for Freedom of the Press, 2012). The section below outlines key features of all-party consent laws that are relevant to psychology researchers interested in sampling social environments.

Many states address electronic modes of communication—email, text messages, and non-public online communication—in their recording laws. Language in most states' laws does not specify exact modes of communication but instead make broad statements seemingly intended to include all electronic communication. For example, Florida's law details that all parties must consent to "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature" (Fla. Stat. § 934.02), whereas Michigan's law broadly states that it applies to "electronic communication using any device" (Michigan Penal Code § 750.539c). Though they use different language, the research implications are the same: Researchers in

some all-party consent states might not be able to legally collect electronic communication from participants without the consent of all parties. Further, when electronic communication takes place across multiple states, federal law may also be relevant, and should be consulted. Check with your own legal counsel for how to ensure legal collection of social environment sampling data.

Reasonable Expectation of Privacy Exception. Many of the all-party consent states include an important exception to the recording laws (one-party consent state laws may also contain this exception): One need only obtain all parties' consent for conversations in which people have a reasonable expectation of privacy (e.g., California Penal Code § 632). This exception stipulates that conversations held in public places, where people cannot reasonably expect privacy, can legally be recorded without consent. State courts have generally interpreted "reasonable expectation of privacy" as settings in which interactions take place where one cannot easily be overheard by most people, without the aid of an amplification device (Reporters Committee for Freedom of the Press, 2012). However, this clause can be interpreted differently among legal experts, so be sure to consult your own legal counsel.

Public versus Private Communication. "Reasonable expectation of privacy" necessarily brings up questions regarding what constitutes public versus private communication, and what is reasonable. Unfortunately, there is no single answer to these questions (Sanders, supra, 20 Cal. 4th). Buchanan and Williams (2010) detail ethical guidelines, which are discussed in more detail in "Ethical Considerations."

Visual Recording. State laws vary as to whether recording laws apply to photographs and video. In some all-party consent states, photographs and videos may only be recorded with

all parties' consent in any context that confers a reasonable expectation of privacy (akin to that described in audio recording). Other all-party consent states (surprisingly, not all one-party consent states) only outlaw taking photographs and videos in *very* private settings and manners, when the goal or end result is to capture nudity without consent. These laws were enacted specifically to combat nonconsensual "up-skirt" or "down-shirt" photographs, or in places where nudity is expected or common, such as in public restrooms (See In re Deborah C., 635 P.2d 446, 1981).

Social Media. The term "electronic communication" could certainly be interpreted to apply to Facebook and Twitter accounts, for example, that use "private" rather than "public" settings. At least one state court (New Jersey) has ruled that electronic communication includes social media (Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 661 [D.N.J. 2013]; Wright, 2013). In any case, "private" content will likely require the consent of at least one participant in the online communication. In social media studies where users typically consent to provide information to researchers, but posts and comments made by bystanders—"friends" or "followers"—may have an expectation of privacy if their accounts are not public. A few sources shed light on ways in which privacy applies to social media content (Student Press Law Center, 2016). For example, Facebook's Terms of Service, to which all users consent, includes statements that content will be stored by Facebook and may be shared with advertisers, new owners, and "third party companies" (Facebook Data Policy, 2015). These policies may undermine a reasonable expectation of privacy. Beyond the Terms of Service, people often "friend" hundreds of people on their Facebook accounts, making it questionable

whether communication intended to be visible to hundreds of people could be considered "private."

Intrusion upon Seclusion and Trespass Laws

Legal liability with social environment sampling may also extend to intrusion upon seclusion and trespass laws. Intrusion upon seclusion law states that "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs… is subject to liability… if the intrusion would be highly offensive to a reasonable person" (Restatement [Second] of Torts § 652B). Likewise, trespass law entails "the act of knowingly entering another person's property without permission" (Staff, 2007). In both laws there is a requirement for *intent* to invade one's privacy. Thus, these may only apply to social environment sampling if the data is obtained surreptitiously. Participants and researchers should be particularly cautious when recording data on private property, and carefully consult legal counsel.

Ethical Considerations

Researchers are of course bound to ethical standards that extend beyond what is legal. The sections below outline some ethical considerations for social environment sampling. For many of the issues mentioned here, there is not one solution that will resolve each ethical issue with social environment sampling methods. The purpose of this section is to raise questions psychology researchers should keep in mind when designing their studies.

Consent

Kraut and colleagues (2004) described appropriate considerations for consent in online research. In some cases, principles applied to online research apply to other social environment

sampling methods. The most relevant considerations include whether or not: 1) bystanders are human subjects, 2) bystanders' data is observation of publicly available data or is unidentifiable, 3) bystanders are subject to more than minimal risk, 4) it is practical to obtain documented consent, 5) obtaining documented consent from bystanders would introduce risk by creating an identifying link to their data.

Public versus Private Behavior

Perceptions of privacy are context dependent, and need to be considered for each social environment sampling method and the context in which it is used. For example, people using a publicly available support forum for managing a chronic illness may have greater expectations of privacy than someone posting a photo on a public Facebook account. Some people might even expect their public behavior to remain private (E. A. Buchanan, 2011). Some scholars believe that expectations of people who post information online—which might extend to publicly observable behavior—matter beyond what is reasonable for them to expect (T. Buchanan & Williams, 2010). It is the author's position that these issues should be considered within reason. It is important to consider the potential harm done: Might the research interfere with users' interaction with a social media site? Will recorded audio or visual records of an interaction or behavior negatively affect a bystander's life? Who is liable if data is recorded illegally?

Confidentiality

All human subjects data must be stored securely, but social environment sampling also requires attention to transmitting or downloading data securely (T. Buchanan & Williams,

2010). Researchers should consider whether the data need to be transmitted via the internet, and if so, security of the connection should also be considered.

After the data are obtained, is it possible to identify participants through information in the study report? Would a quote from an audio file or social media interaction, or a photo from a lifelogging study be identifiable if included? What specific demographic information is necessary to report, and will it make participants identifiable (Zimmer, 2010)?

Practical Suggestions for Research

There is no set of solutions that will resolve all legal and ethical concerns with social environment sampling methods; however, this section will present some practical solutions that may each resolve multiple legal or ethical concerns. Some solutions are common across social environment sampling methods. In general, all data should be de-identified at the earliest possible opportunity in the research process. Further, because they entail use of technology, researchers must consider whether or not they need to connect to the internet or store data on a cloud. This could introduce potential weakness for data security, and therefore should only be used when necessary. For example, social media necessitates an internet connection, but data gathered can be stored offline. Methods like the EAR may store data locally on password-protected devices until researchers download it. Some devices (e.g., iPods) provide the opportunity to delete data if the wrong password is entered 10 times, adding another layer of security.

After data collection, research assistants typically process data, coding for psychologically-relevant constructs. When data is collected and processed in the same city, it is possible that participants may be identified by research assistants. In this event, research

assistants should immediately notify the principal investigator, and be switched to another participant.

Audio Recording

This section focuses on solutions for the EAR, but could also apply to similar audio-recording methods (e.g., LENA; Ramirez-Esparza, Garcia-Sierra, & Kuhl, 2010). EAR study protocols generally instruct participants to wear the device visibly on their clothing and tell others about the potential to be recorded. This is a first step in removing reasonable expectation of privacy. Of course, as participants engage in their daily activities, they may forget to inform people with whom they interact that they may be recorded. Therefore, the author developed a potential solution for EAR research in California, which may be adapted for use in other all-party consent states. Because the EAR is designed to sample people's social behavior and environments, and it is infeasible to consent all people with whom a participant interacts over the course of a monitoring period (usually a weekend), solutions must automatically remove expectation of privacy when interacting with EAR participants. The EAR records only the participant's side of phone conversations, so solutions need not extend to this context. Therefore, the only people who need to be warned of the potential to be recorded are those who interact with EAR participants face-to-face. Following consultation with lawyers and the Institutional Review Board (IRB) at the author's institution, a solution was deemed appropriate:

Figure 1. The EAR and bystander button

Participants would visibly wear a button stating “this conversation may be recorded” and displaying an image of a microphone (Figure 1). Participants are instructed to wear the button, and told why it is important in complying with California state law. To reinforce the importance of wearing the button, the consent form includes a checkbox that prompts participants to indicate they understand the need to wear the button and explicitly agree to wear it. These materials are available on the EAR Open Science Framework (OSF) website (https://osf.io/n2ufd/; Robbins, Wright, Karan, & Baranski, 2016).

Lawyers at the author’s institution concluded that this combination of solutions is appropriate for removing a reasonable expectation of privacy, though legal opinions can widely vary. Although public conversations are not typically not considered private, one could imagine scenarios in public places where people might have a reasonable expectation that their conversation is private. For example, a small group speaking quietly in a restaurant booth may reasonably assume that no one could overhear them. If one member of the party is participating in an EAR study, wearing the button should remove conversation partners’ expectation of privacy. However, if people in a nearby booth are speaking loud enough that one can overhear without aid, then those people may not have a *reasonable* expectation of privacy (Reporters Committee for Freedom of the Press, 2012) and may not need to see of the button to be recorded legally.

Manson and Robbins (under review) provide empirical evidence for the effective implementation of the bystander button. They found that participants reported bystanders noticed the EAR or button (M = 3.0) and talked about them (M = 3.2), but that this generally did not impede their daily activities (M = 1.4; all on a 5-point scale).

Participants can also pause the EAR if a bystander objects to being recorded or if the participant wants a particular event to remain private. Researchers enable this function when they program the EAR, and they can specify how long the device will pause. Participants can press the button as many times as needed to keep a conversation private.

Data from the author's ongoing study of 55 healthy adult couples reveal that 21.8% of participants used the button (n=24), but very few sound files scheduled to record were prevented from recording due to the pause button (0.1%). Among the monitored weekends in which the pause button was used, the average number of pauses was 2.7 (SD = 2.8). Participants used the pause function, but it did not impede data collection.

Researchers may be concerned about missing the information omitted as a result of the pause button, but the option is parallel to participants skipping a question they do not want to answer on a questionnaire, or removing the device. Ultimately, participants must be comfortable with the information they provide to researchers.

These practices may facilitate the legal collection of sound data in all-party consent states—subject to legal interpretation. However, in more restrictive states lacking an exception for non-private, in-person conversations, legal counsel may determine that these suggestions are insufficient. One solution is to have participants only wear the EAR at home or in another target location (e.g., workplace) where researchers could plausibly obtain consent from all relevant parties.

Three procedures can be enacted after sound files are collected to further secure participants' and bystanders' privacy and confidentiality. First, participants have the opportunity to listen to and delete any sound files they or a conversation partner wish to

remain private before researchers access them. Second, if any sound file contains personally identifying information, the researcher removes this information using a sound editor (several are freely available online and fairly intuitive to use). Third, as mentioned above, if a research assistant recognizes a participant's voice, they are immediately switched to coding another participant.

These procedures for EAR research have been deemed ethical by the author's and several IRBs' standards. EAR research has been conducted in this manner (minus the bystander button) at the University of Arizona, University of Missouri, University of Texas, and Washington University in St. Louis, among others. These procedures, with the addition of the bystander button, have been approved at the University of California (Riverside and Los Angeles) and Stanford University. Thus, some degree of consensus regarding the ethical nature of EAR data collection has been reached. Most importantly, for over a decade of EAR research, no participants have reported adverse events regarding their own or bystanders' privacy. These data support the notion that risks involved with conducting such research are low.

Visual Recording

In states where all-party consent is required in non-public places, it would be very difficult to implement a lifelogging study that uses a device like Narrative (Brown & Sherman, under review). Because these devices are worn by participants and take pictures automatically, bystanders' images would certainly be recorded. A bystander button like the one used for EAR research would not suffice to inform people they may be photographed if they are not near the participant. A person may be visually identifiable in a picture or video even at a distance and facing away from the picture-taker. This makes legal issues trickier than with audio-recording,

which generally only captures people who are very near to the participant (or talking at such a loud volume that they do not expect privacy). Researchers could ask participants to take the device off in private settings, but this may be burdensome for participants, and they are likely to forget to remove it in some circumstances. In states where it is only legal to capture visual data with all parties' consent, it would be insufficient to ask participants to review and delete photos, because taking the photos or videos in the first place is illegal (See In re Deborah C., 635 P.2d 446, 1981). Unfortunately, it simply may not be feasible to run such a study in these states.

Researchers should consider several procedures to ethically implement studies employing lifelogging techniques (video and photo). Once researchers obtain data, they can blur faces of bystanders and erase the original images so they will never be seen after that early stage. When possible, participants could also be encouraged to seek verbal consent from people with whom they interact (Kelly et al., 2013). Narrative has privacy features so participants can stop recording for a set period of time if anyone requests privacy. The cameras can also be easily turned around, covered, or removed. These practices are common and have been successful at protecting participants' and bystanders' privacy (Brown & Sherman, under review).

Brown and Sherman (under review) present data with a scale identical to that used for the EAR, adapted for Lifelogging methods. Like the EAR findings mentioned above, participants reported bystanders were somewhat aware of the narrative (*M*=3.2) and talked about it (*M*=3.0), but it did not substantially impede their daily activities (*M*=1.4; all on a 5-point scale).

Electronic Communication

Solutions for collecting electronic communication can be challenging due to the variety of contexts in which they take place. When feasible, it is ideal to obtain consent of all parties to the communication, but in many cases this requirement would be too burdensome. Further, such studies often contribute knowledge that outweighs the privacy risks associated with deidentified analysis of communications when at least one person has consented to data collection. For example, researchers have developed online interventions to improve well-being (Eysenbach, Powell, Englesakis, Rizo, & Stern, 2004; Ryan, Shochet, & Stallman, 2010).

The safest approach to legally and ethically collect electronic communication data in states with restrictive laws would be to limit data to messages between explicitly consenting parties (e.g., mentor and mentee, members of a family). All parties would not necessarily be participants but could provide consent to disclose their electronic communication. Participants could then provide researchers with the electronic communications between consenting parties.

In some cases it may not be practical for participants to identify and provide all relevant communications. In these cases, researchers need a way to search participants' electronic communications for messages between consenting parties without violating the lack of consent by other parties. One solution is to target participants' outgoing messages to avoid collecting communication by non-consenting parties (e.g., Pennebaker, Groom, Loew, & Dabbs, 2004). Text and instant messaging provide easier formats for targeted message collection between specific parties, relative to email, as most smartphones and chat programs organize communication by user. Researchers who wish to include electronic communications in their data collection should keep a close eye on privacy law developments in their state.

Recommendations have been developed for conducting ethical social media research and may extend to other electronic communication. Social media users' awareness that a platform's terms include storing and sharing their data may not necessarily extend to consent for their data to be used for research. Therefore, bystanders' privacy and confidentiality should be carefully considered. First, data should be deidentified to the fullest extent possible, as soon as possible, to ensure privacy at all subsequent stages of research and analysis.

Second, researchers should exercise caution when publishing direct quotes from social media data. Even deidentified quotes may become identifiable if they are indexed by search engines, making it possible to attribute the quote to its author. Though this may only apply to online data that is made public in the first place, researchers should consider whether the poster's reputation might be altered as a result of it being used for their particular analysis (e.g., use of "I" and narcissism; Carey et al., 2015).

Third, researchers can ask participants to provide anonymized emails when practical (e.g., Kacewicz, Pennebaker, Davis, Jeon, & Graesser, 2013). For larger-scale analyses, automating the analysis of deidentified electronic communication (e.g., via word-count software or social language network analysis; e.g., Scholand, Tausczik, & Pennebaker, 2010) rather than using human coders is likely to pass most ethical standards.

Other suggestions for handling electronic communication data draw from guidelines for clinical research data. Clinical researchers may use existing medical records without consenting patients "if the material is anonymised at the earliest possible stage, if there is no inconvenience or hazard to the subjects, and if the institutional review board has reviewed and agreed the research protocol" (p. 1104; Eysenbach & Till, 2001; National Institutes of Health,

2004). Likewise, potential harm is an important consideration for social media and other electronic communication data. If researchers store data in a secure and confidential manner, and direct quotes are not attributable to their source, the research is unlikely to pose much of a risk to participants or bystanders.

Caveats

These solutions may be too restrictive in some cases, and not restrictive enough in others. When handling social environment sampling data from sensitive populations, it is possible to observe information that would be particularly damaging to someone if there were a breach of confidentiality or privacy. For example, a participant who attends Alcoholics Anonymous® meetings could potentially expose bystanders' identity in a context where anonymity is a central tenet. On the other hand, the proposed solutions could be counterproductive or unnecessary in samples where there is particularly low risk, or where state laws only require one-party consent to recording observable information. The author agrees with Kraut and colleagues (2004) that "no purpose is served when researchers or their IRBs place hurdles in front of research involving minimal risk" (p. 114). Use of materials should be appropriate for the sample, with increased protections when studying sensitive populations, and eliminating excessive procedures when risks are minimal.

Social Environment Sampling and the IRB

Educating Your IRB

When IRBs are unfamiliar with social environment sampling methods, they may (understandably) err on the conservative side to protect participants, bystanders, and their institution. Thus, it is critical for researchers to educate their IRB about the methods and

surrounding legal and ethical issues from the start. Providing an IRB with the information presented here, in addition to your own research, before submitting a protocol for approval is likely to foster a collaborative spirit for developing feasible solutions to legal and ethical challenges associated with social environment sampling. For example, the author met with her IRB chair before submitting her first EAR study protocol, and always includes the relevant law as an appendix in IRB applications, highlighting relevant portions. She also includes a clear definition of the "reasonable expectation of privacy" and why practices delineated earlier reasonably remove this expectation.

The EAR OSF for Sample Materials

Sample IRB materials that the author has used for EAR protocols at the University of California, Riverside are on the EAR OSF page (https://osf.io/n2ufd/; Robbins et al., 2016). Researchers should modify them as needed to comply with relevant state laws. The vendor and design code for the author's bystander button are also freely available there (though one could design and purchase them elsewhere).

Conclusions

This paper outlines the legal and ethical issues that researchers must consider when conducting social environment sampling research. Though not exhaustive, this guide can facilitate best research practices when collecting audio, visual, electronic, and social media data from everyday life. Researchers should not view these practices as static or definitive, given the rapidly changing technological and associated legal landscape. It is important to consider the ethical practices of social environment sampling research in light of the public's ever-changing expectations for privacy and what is deemed "normal."

The capabilities offered to psychology researchers by new technology have catapulted the field toward a deep understanding of people's experiences and social environments. Yet, this potentially great payoff comes with more responsibility on researchers to stay up-to-date on relevant laws and actively consider the best ethical practices within the bounds of the law.

References

Anderson, B., Fagan, P., Woodnutt, T., & Chamorro-Premuzic, T. (2012). Facebook psychology: Popular questions answered by research. *Psychology of Popular Media Culture*, *1*(1), 23.

Barker, R. G., & Wright, H. F. (1951). *One Boy's Day; A Specimen Record of Behavior*. Oxford, England: Harper.

Ben-Zeev, D., Wang, R., Abdullah, S., Brian, R., Scherer, E. A., Mistler, L. A., … Choudhury, T. (2016). Mobile Behavioral Sensing for Outpatients and Inpatients With Schizophrenia. *Psychiatric Services*, *67*(5), 558–561. https://doi.org/10.1176/appi.ps.201500130

Brown, N., & Sherman, R. (under review). A snapshot of the life as lived: Lifelogging in social and personality psychological science.

Buchanan, E. A. (2011). Internet research ethics: Past, present, and future. *The Handbook of Internet Studies*, *11*, 83.

Buchanan, T., & Williams, J. E. (2010). Ethical issues in psychological research on the internet. In S. D. Gosling & J. A. Johnson (Eds.), *Advanced Methods for Conducting Online Behavioral Research* (pp. 255–271). Washington, DC: American Psychological Association.

Carey, A. L., Brucks, M. S., Küfner, A. C., Holtzman, N. S., Back, M. D., Donnellan, M. B., … others. (2015). Narcissism and the use of personal pronouns revisited. *Journal of Personality and Social Psychology*, *109*(3), e1.

Eysenbach, G., Powell, J., Englesakis, M., Rizo, C., & Stern, A. (2004). Health related virtual communities and electronic support groups: systematic review of the effects of online peer to peer interactions. *Bmj*, *328*(7449), 1166.

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *BMJ*, *323*(7321), 1103–1105. https://doi.org/10.1136/bmj.323.7321.1103

Facebook Data Policy. (2015). Retrieved August 10, 2016, from https://www.facebook.com/about/privacy/

Hodges, S., Berry, E., & Wood, K. (2011). SenseCam: A wearable camera that stimulates and rehabilitates autobiographical memory. *Memory*, *19*(7), 685–696.

Kacewicz, E., Pennebaker, J. W., Davis, M., Jeon, M., & Graesser, A. C. (2014). Pronoun use reflects standings in social hierarchies. *Journal of Language and Social Psychology*, *33*, 125–143. https://doi.org/10.1177/0261927X13502654

Kelly, P., Marshall, S. J., Badland, H., Kerr, J., Oliver, M., Doherty, A. R., & Foster, C. (2013). An ethical framework for automated, wearable cameras in health behavior research. *American Journal of Preventive Medicine*, *44*(3), 314–319.

Kraut, R., Olson, J., Banaji, M., Bruckman, A., Cohen, J., & Couper, M. (2004). Psychological research online: report of Board of Scientific Affairs' Advisory Group on the Conduct of Research on the Internet. *American Psychologist*, *59*(2), 105.

Matthiesen, B. W., Wickert, G. L., & Lehrer, D. W. (2016). Laws on recording conversations in all 50 states. Retrieved from https://www.mwl-law.com/wp-content/uploads/2013/03/LAWS-ON-RECORDING-CONVERSATIONS-CHART.pdf

Mehl, M. R., & Conner, T. S. (Eds.). (2012). *Handbook of Research Methods for Studying Daily Life*. New York, NY: Guilford Press.

Mehl, M. R., Gosling, S. D., & Pennebaker, J. W. (2006). Personality in its natural habitat: manifestations and implicit folk theories of personality in daily life. *Journal of Personality and Social Psychology*, *90*(5), 862.

Mehl, M. R., & Pennebaker, J. W. (2003). The sounds of social life: A psychometric analysis of students' daily social environments and natural conversations. *Journal of Personality and Social Psychology*, *84*(4), 857–870. https://doi.org/10.1037/0022-3514.84.4.857

Mehl, M. R., Pennebaker, J. W., Crow, D. M., Dabbs, J., & Price, J. H. (2001). The Electronically Activated Recorder (EAR): A device for sampling naturalistic daily activities and conversations. *Behavior Research Methods, Instruments, & Computers*, *33*(4), 517–523.

Mehl, M. R., Robbins, M. L., & Deters, F. große. (2012). Naturalistic observation of health-relevant social processes: The Electronically Activated Recorder (EAR) methodology in psychosomatics. *Psychosomatic Medicine*, *74*(4), 410–417. https://doi.org/10.1097/PSY.0b013e3182545470

Mehl, M. R., Vazire, S., Ramírez-Esparza, N., Slatcher, R. B., & Pennebaker, J. W. (2007). Are women really more talkative than men? *Science*, *317*(5834), 82–82.

Miller, G. (2012). The smartphone psychology manifesto. *Perspectives on Psychological Science*, *7*(3), 221–237.

National Institutes of Health. (2004). HIPAA Privacy Rule and Its Impacts on Research. Retrieved August 12, 2016, from https://privacyruleandresearch.nih.gov/clin_research.asp

Pennebaker, J. W., Groom, C. J., Loew, D., & Dabbs, J. M. (2004). Testosterone as a social inhibitor: two case studies of the effect of testosterone treatment on language. *Journal of Abnormal Psychology*, *113*(1), 172.

Ramirez-Esparza, N., Garcia-Sierra, A., & Kuhl, P. K. (2010). Naturalistic social communication and speech development in monolingual and bilingual infants. *The Journal of the Acoustical Society of America*, *128*(4), 2459–2459.

Reporters Committee for Freedom of the Press. (2012). Reporter's recording guide: A state-by-state guide to taping phone calls and in-person conversations. Retrieved May 23, 2016, from http://www.rcfp.org/rcfp/orders/docs/RECORDING.pdf

Restatement of the Law, Second, Torts, § 652. (n.d.). Retrieved December 12, 2016, from https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm

Robbins, M. L., López, A. M., Weihs, K. L., & Mehl, M. R. (2014). Cancer conversations in context: Naturalistic observation of couples coping with breast cancer. *Journal of Family Psychology*, *28*(3), 380–390. https://doi.org/10.1037/a0036458

Robbins, M. L., Wright, R. C., Karan, A., & Baranski, E. (2016). EAR Repository. Retrieved August 1, 2016, from https://osf.io/n2ufd/

Ryan, M. L., Shochet, I. M., & Stallman, H. M. (2010). Universal online interventions might engage psychologically distressed university students who are unlikely to seek formal help. *Advances in Mental Health*, *9*(1), 73–83. https://doi.org/10.5172/jamh.9.1.73

Scholand, A. J., Tausczik, Y. R., & Pennebaker, J. W. (2010). Social language network analysis. In *Proceedings of the 2010 ACM conference on Computer supported cooperative work* (pp. 23–26). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1718925

Slatcher, R. B., & Pennebaker, J. W. (2006). How do I love thee? Let me count the words the social effects of expressive writing. *Psychological Science*, *17*(8), 660–664.

Staff, L. I. I. (2007, August 6). Trespass. Retrieved December 12, 2016, from https://www.law.cornell.edu/wex/trespass

Student Press Law Center. (2016). When it comes to social media, some old-school legal rules may not apply. Retrieved August 10, 2016, from http://www.splc.org/article/2014/08/when-it-comes-to-social-media-some-old-school-legal-rules-may-not-apply

Sun, M., Fernstrom, J. D., Jia, W., Hackworth, S. A., Yao, N., Li, Y., … Sclabassi, R. J. (2010). A wearable electronic system for objective dietary assessment. *Journal of the American Dietetic Association*, *110*(1), 45.

Tausczik, Y. R., Chung, C. K., & Pennebaker, J. W. (2014). Tracking secret-keeping in emails. *Manuscript under Review*. Retrieved from https://www.terpconnect.umd.edu/~ylatau/files/TausczikChungPennebaker2016.pdf

Worringham, C., Rojek, A., & Stewart, I. (2011). Development and feasibility of a smartphone, ECG and GPS based system for remotely monitoring exercise in cardiac rehabilitation. *PloS One*, *6*(2), e14669.

Wright, P. (2013). Court Finds Non-Public Facebook Posts Are Covered By The Stored Communications Act--But Not Posts Produced By A User's Frenemy | Employer Law Report. Retrieved November 28, 2016, from http://www.employerlawreport.com/2013/08/articles/social-media-2/court-finds-non-public-facebook-posts-are-covered-by-the-stored-communications-act-but-not-posts-produced-by-a-users-frenemy/

Zimmer, M. (2010). "But the data is already public": on the ethics of research in Facebook. *Ethics and Information Technology*, *12*(4), 313–325.

Zimmer, M., & Proferes, N. J. (2014). A topology of Twitter research: Disciplines, methods, and ethics. *Aslib Journal of Information Management*, *66*(3), 250–261.