Chapter 7

Ethical, privacy, and confidentiality issues in the use and application of social media

Amar Kanekar and Joseph Otundo
School of Counseling, Human Performance and Rehabilitation, College of Business, Health and Human Services, University of Arkansas, Little Rock, AR, United States

Learning objectives

After reading this chapter, you should be able to:

1. Define the terms media and social media.
2. Differentiate between privacy and confidentiality in social media-based platform usages, for example, Facebook, Twitter, etc.
3. Explain the terms beneficence, nonmaleficence, and justice as applicable to public health.
4. Discuss the role of ethics in social media usage.
5. Delineate major ethical issues related to social media usage.
6. Appraise the issues arising from the application of social media-based platforms in a research setting.
7. Discuss the literature on the application of privacy and confidentiality issues in social media-based public health studies.

Social media and its varied applications

We are currently living in times where social media has become as ubiquitous as print media in past times. Rarely would you find someone who is unfamiliar with any or all these such as Facebook, Twitter, YouTube, Instagram, and Snapchat. Before we explore the reasons for the rise of these platforms, we need to understand that the basis of having these is the invention of the "Internet." The rise of the Internet over the last several decades has given opportunities for human-to-human interaction via social media such that humans can easily communicate with each other via blogs, applications (called

Effective Use of Social Media in Public Health. https://doi.org/10.1016/B978-0-323-95630-7.00006-8

apps), video conferencing, and digital media (by which we mean platforms called social media (Vriens & Van Ingen, 2018)). Social media is not only a form of entertainment media for consumption, sharing, and producing digital information but also has been of immense application in recent times either for election campaigns, higher education marketing, sports, or as a self-branding tool. These applications of social media in a variety of fields show its growing importance.

Although "media" by definition means a plural term of the word "medium" of cultivation, conveyance, and/or expression (Media, n.d.) and "social" means marked by pleasant companionship with friends and associates (Social, n.d.) separately, "social media" can be defined as "forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages and other content (such as videos)" (Social media, n.d.). This brings to "conversational media" which is "a group of web-based apps used for creating and transmitting content in the form of words, pictures, and multimedia" (Bensley & Brookins-Fisher, 2019).

The purpose of this book chapter is to discuss three specific parameters for social media platform usage: (a) ethics or ethical aspects in social media-based platform usage, (b) privacy issues while using social media-based platforms, and (c) confidentiality and issues revolving around it while using social media-based platforms. Although the authors have categorized these aspects of social media usage, they tend to overlap and cause complexity, while delineating their applications in either personal or professional lives.

To that end, "research ethics" is inbuilt into the application of social media-based platforms while designing and implementing research studies in the public health or health education field. The authors include two case study vignettes to demonstrate these complexities and offer possible approaches to navigate emerging and established issues arising from these applications.

Role of ethics in social media usage

In our current society, the role of ethics is valuable and often tested either when we make decisions for ourselves, or as a part of a group, organization, or society. Some of the common examples would be the role of vaccines and their allocation, end-of-life decisions, and using gene alteration of stem cells. These are controversial topics in society and ethical norms, beliefs, and dilemmas make addressing them a challenging lifelong process. Lines get blurred when the effects of human actions are weighed against what is morally and ethically correct or not when dealing with these issues and their outcomes in terms of the societal effects.

Are "ethics versus morality" interchangeable terms or is there a difference? Let us first see the definition of these two terms. Ethics is broadly defined as a theory or a system of moral values, principles of conduct governing an individual

or a group (Ethic, n.d.), whereas "morality" or "morals" concerns what is right or wrong in human behavior, considered what is a right behavior by most people and agreeing with a standard of right behavior (Moral, n.d.). In the context of health education/promotion, ethics is the science of how choices are made, whereas morality sets standards for right or wrong in human behavior (Cottrell et al., 2023)

Why do we need to behave ethically as humans? One of the reasons we need to behave ethically is it provides us a sense of purpose and meaning (references) to one's life, particularly as one functions and thrives in a vibrant society. It's the right thing to do no matter what. There are numerous ethical theories such as *deontology* (also known as formalism or nonconsequentialism) where the primary reasoning is that the end does not justify means and *teleology* (also known as consequentialism) where the primary reasoning is that the end does justify the means. We will be seeing the application of these theories in the context of social media usage in the latter part of this section. But before we discuss the theories and their applications, particularly in terms of the use and application of social media in professional and research settings, we need to discuss the fundamental realms of ethics: (a) professionalism or professional ethics and (b) research ethics (Cottrell et al., 2023).

Professionalism and the role of professional ethics are extremely important, particularly when professionals use social media either for professional reasons or just for social purposes. Often professionals either get confused or are not fully versed in the balance between maintaining their identities in a professional environment versus a social environment and lines often get blurred. Maintaining and updating one's identity on a social media platform is as vital as in a professional platform (e.g., LinkedIn), as any kind of expression of morally inappropriate behavior whether, through sharing of information (textual, images, or videos), consumption of information (textual, images, or videos), or building of information (via groups or webpages) on social media-based platforms can adversely affect one's reputation and societal image. For example, a professional may post textual comments which could be religiously or politically offensive and hence may adversely affect the person's professional reputation and his work.

As per the Belmont Report which was the basis for the revision of 45CFR46-the common rule, the core ethical principles which govern ethical functions include beneficence and nonmaleficence, justice, and respect for persons (U.S Department of Health & Human Services, 2021). These principles when applied to social media usage can be discussed as follows:

Beneficence deals with maximizing the good and minimizing harm. There is an obligation to protect persons by creating and sharing content that provides maximum good and minimizes harm. In the context of social media usage, it would be expected that content creators of messages, stories, news, images, and pictures share the information being mindful that these do not harm readers in a reasonable manner, for example, sharing inappropriate and

unrealistic body images and pictures of social gathering with excessive alcohol usage should be minimized or nonexistent (Tseng et al., 2019).

Nonmaleficence indicates doing no harm to the study participants. An area that gets challenging for social media platforms is advertisers which can make false advertising via social media and entice subscribers to buy things or sharing of fake news which can create inappropriate messaging and adds fuel to the fire (Relihan, 2018). Some of the strategies for counteracting this deal with banning and regulating false advertisements along with setting up diverse filters for regulating fake news (Kanekar & Thombre, 2019). It is strongly recommended that healthcare organizations, particularly public health organizations counter these practices with authentic evidence-based messages.

Justice, particularly, in the context of public health means fair deliberative procedures and equitable distributions of burdens and benefits. Social media-based studies inherently compromise justice to a major extent as those without a social media account do not get an opportunity to voice their opinions, thoughts, and attitudes. On the flip side, justice can be invoked by using social media as an advocacy tool to advocate for social justice (Fileborn, 2017). This is highly encouraged for public health justice.

Respect for persons can be initiated by having an informed consent document or a statement that introduces the social media-based study participants to the study and seeks their consent with a "yes" and "no" button to participate. Researchers and coinvestigators of a social media-based study should be aware that all posts seen on social media are not necessarily "public data" (most tweets on Twitter are "public" and some spaces and groups could be private [e.g., closed groups in Facebook and private one on one discussions in Twitter]) which need detailed informed consent either from the social media study participants or the administrator or gatekeeper of a social media-based group.

Role of privacy in social media usage

By definition, "privacy" means freedom from unauthorized intrusion and has an element of secrecy (Privacy, n.d.). When we think of social media applications such as Facebook, YouTube, Twitter, and Instagram, they all have "privacy" built into the user interface as part of the navigational settings. For instance, Facebook has quite detailed "privacy" settings which involve a variety of aspects such as "password" protection, 2-step authenticity verification, and content visibility to users as well as those who would access the content generated by users (such as availability of content to friends, friends of friends, and/or the general public). Similarly, a cursory glance at "YouTube" settings would indicate to media disseminators that one can keep one's playlists and subscriptions private or available to the public.

The social media platform "Twitter" has an extensive privacy setting where a Twitter user has adequate control over aspects of managing the information associated with tweets, managing the contacts and the visibility of the

message, the consumption of the content along with the advertisements seen, and finally data sharing and connection with other businesses. The privacy policy of Twitter is very detailed and useful for anyone wanting to use Twitter for information consumption or information dissemination (Twitter, 2022).

Although all of the social media-based platforms have a privacy policy for intended users, it would be good and beneficial for researchers to train themselves and be aware of these policies prior to embarking on using social media platforms or applications as tools in the participant recruitment process and data collection. Ideally, it would be highly beneficial if the Institutional Review or Ethics review boards at institutions have some guidelines developed for maintaining privacy when it comes to social media-based research. This could be instituted in the manuals and websites designed by the Institutional Review Boards (IRBs) and/or via videos or modules which discuss the importance and implications of "privacy" when conducting social media-based research (for the participants as well as the researcher).

Sometimes it could be the role of a researcher or the study investigator to provide the participants with useful information on their rights as a participant in the social media-based study, for example, an investigator may ask the participant to familiarize themselves with the public versus private guidelines of a social media platform (such as Facebook or Twitter) before they commit to their participation in the study. Alternatively, the consent form for the proposed study could include specific language which attests that the participants are aware of whether their information would be either public or private before they engage actively with the social media platform.

Although participant privacy may be controlled at the researcher level along with oversight by the IRB, there can certainly be instances where there could be opportunities for risks. Thus, both the participants and non-participants could be affected such as third-party risks. For example, asking questions via social media-based blogs or platforms for a family-focused issue may protect research participants but not the participants' immediate family members. This can happen in a quantitative, qualitative, or mixed-methods research approach (Office for Human Research Protections, 2021). Therefore, it is suggested that the researchers or coinvestigators include a plan of how they would be addressing this, particularly when they use social media platforms for recruitment and data collection. This could be an additional protective layer for maintaining the "privacy" of participants.

The distinction between what would be "private" versus what would be "public" in research needs some discussion. "Private" information in the context of Internet-based information would be where an individual's behavior is reasonably expected to not be made public by the individual via observation or recording. This could be further clarified in terms of being a research participant where the identity of a participant can be readily ascertained via the associated information, that is, the information shared, and the identity can be linked.

If the individuals intentionally post textual materials or multimedia on the social media platforms, then it could be presumed to be public unless the platform has privacy or additional policies which preclude that (UA Little Rock Research Protection Program Policies and Procedures, 2018). Although, this is a bit easier when social networking sites mention what is public and what is private, often this information is hidden in deeply seated pages of the social media platform such as Facebook or Twitter and needs to be searched via the networking tools. Furthermore, a research participant may either forget that their profile is set up "publicly" or "privately" or "restricted for friends only" on platforms such as Facebook. This can create a lot of ambiguity for the participant as well as the researcher.

Let us see a couple of examples of how "public" versus "private" is distinguished on two of the popular social media platforms: Facebook and Twitter: Facebook collects a lot of information from its subscribers such as networks, information on product transactions, and even if a subscriber makes his data "private," it is still available to the company. Facebook policies clearly mention that "public" information can be seen by anyone, on or off our products, even if they don't have an account. These include Facebook username; any information shared with a public audience; information in individual profiles on Facebook (Facebook Help Center, n.d.); and content shared on Facebook Page, such as Facebook Marketplace. In addition, people that use Facebook and Instagram can provide access to or send public information to anyone on or off the company products, including other Meta Company Products, search results, or through tools and application programming interface (APIs). Public information can also be seen, accessed, reshared, or downloaded through third-party services such as search engines (like Google), APIs, and offline media such as TV, and by apps, websites, and other services that integrate with our Products (Meta Privacy Center, 2022). So, subscribers need to be aware of these policies when they share information and have not made a specific concerted effort to make their information "private." Another piece of confusion lies in the fact that though the Facebook subscribers can intentionally make their contributions "public," they do not assume that a researcher may use this information for research purposes, but it can be reasonably assumed by a researcher that this information is for "public" use unless the creators or sharers of this information object to it. Hence social media-based data collected via screen capture of Facebook profiles made "public" should and could be considered in the public domain for most cases. If a researcher or a coinvestigator of a research study involving screen capture data is unsure whether the "privacy" aspects of the study are violated, need to consult the IRB at their institution and/or seek oversight on the research process.

Twitter, another social media platform that is widely used for sharing content via short tweets, discussions, and other media sharing has a detailed "privacy" policy. Twitter privacy policy clearly states that "Most activity on Twitter is public, including your profile information and your display language

when you created your account, and your Tweets and certain information about your Tweets like the date, time, and application and version of Tweet. The privacy policy states that subscribers may choose to publish their location in their Tweets or their Twitter profile. When subscribers share audio or visual content using the Twitter platform, the data generated is used for their services for example by providing audio transcription. The lists created by subscribers, people they follow and who follow them, and Tweets such as 'like' or 'retweet' are also public. If subscribers 'like', 'retweet', 'reply', or otherwise publicly engage with the Twitter advertisement services, the advertiser might thereby learn information about subscribers associated with the advertisement. Furthermore, broadcasts (including Twitter Spaces) created by subscribers to the Twitter platform are public along with the information about the date when it was created" (Twitter, 2022).

A subscriber's engagement with broadcasts, including viewing, listening, commenting, speaking, reacting to, or otherwise participating in them, either on Periscope (subject to your settings) or on Twitter, is public along with when they took those actions. On Periscope, for example, hearts, comments, the number of hearts received, and whether a live broadcast was watched or replayed. Any engagement with another account's broadcast will remain part of that broadcast for as long as it remains on the Twitter services. The information posted about you (as a subscriber) by other people who use Twitter services may also be public. For example, other people may tag a photo (if your settings allow it) or mention you in a Tweet. So again, when a researcher captures twitter data via screen capture or through "Twitter analytics" on several tweets or retweets, this information is presumed to be in the "public domain" unless it is specifically hidden by making specific private settings by the user (Twitter, 2022).

"Direct messages" is a Twitter tool that allows more control over privacy and allows users to have nonpublic conversations, protect their tweets, and/or host private broadcasts. Data collected via this tool are subject to "privacy laws" and will need an IRB approval or insight if researchers wish to use any of this for their research studies (Twitter, 2022).

As social media usage continues to rise among professionals, the lines between what is acceptable to share via social media versus professional media (such as LinkedIn-www.linkedin.com) continue to blur and cause confusion. Higher Education faculty is one of such "special groups" of individuals who struggle with maintaining this balance. Due to insufficient guidelines for social media policy usage across most of the institutions of higher learning across the world (Buraphadeja, & Prabhu, 2020), it is up to the individual faculty to find an appropriate balance between their professional and personal lives when it comes to sharing information, opinions, images, and other forms of multimedia via the social networking sites. E-professionalism in essence deals with maintaining a professional identity and expression of traditional professional paradigms through digital media (Cain & Romanelli, 2009).

Although Facebook, Instagram, and YouTube (owned by Google) are the social media platforms that have been very popular over the last few years, it is important to understand that "Snapchat" and "TikTok" are generally popular social media platforms, particularly for generating and sharing user-initiated and created video contents and avatars. These provided instant recognition and a brief sense of fame to the younger generation at the expense of losing their rights for content creation to the companies that own these (Johnston, 2020). Although YouTube videos are distinct from other social media outlets where an individual can make the video availability settings private versus public, data shared through Facebook can be shared to WhatsApp and Instagram as these are sister apps. So, although one can technically delete one's account on one of the platforms such as Facebook, Instagram, and/or WhatsApp, the data could be shared through another platform as per the terms and agreements of these platforms (belonging to one family). Furthermore, even if one deletes one's account, the information shared by others about you are not deleted (Karlis, 2019). This can have deleterious effects related to maintaining confidential information.

The use of social media in teaching is fraught with concerns from faculty as well as students. Faculty professionals are mainly concerned with privacy issues when sharing course information or having student interactions and are involved in mainly sharing YouTube videos passively. Videos subscribed via "YouTube" accounts can be made public by changing the preference in the settings and choosing "private subscriptions" via an individual account (https://www.youtube.com/account_privacy); similarly, while creating videos on YouTube, one needs to use the "YouTube creator studio" and pick the advanced setting of this tool, particularly if one is sharing educational videos to children (these are protected by the Children's Online Privacy Protection Act [COPPA]) (Fruhlinger, 2021). Hence, it is important to be aware of what information is collected or shared via "YouTube" usage as a social media tool, as governed by laws and regulations. While students have mixed feelings about the use of social media in the school context as seen in a recent study, which also reiterated the original use of social networking space more as a tool for social networking among family and friends (Dennen, & Burner, 2017).

Some of the recommendations involve being aware of one's professional identity and how to carefully cultivate one's presence on social networking sites such that the digital footprints left demonstrate mindfulness of positive social behaviors and engagement in ethical behaviors while creating and disseminating content and/or opinions via the social networking sites. This also extends to initiating and maintaining relationships with peers via social networking sites through communication (such as tweets) or through engagement via online support groups hosted by social media platforms such as Facebook and Twitter (Forbes, 2017). Professionals and students need to be mindful that most of the information shared via social media platforms can be used by anyone accessing their profiles through public search engines unless

they have specifically requested that information to be hidden from a "public view."

Case study 1: Facebook-based research study

A researcher at a mid-western University wanted to conduct a research study about support mechanisms in a breast cancer support group (for participants who had a recent diagnosis or are in remission) that is hosted on Facebook. It is expected that participants in this support group would be sharing their thoughts, feelings, and opinions about breast cancer diagnosis and issues related to that. The researcher wants to approach this group for data collection as one of the researcher's primary research questions is what does the diagnosis of breast cancer mean to the participants?

Case study questions

1. Does a researcher need any kind of training to pursue such as research study?
2. What would be the approaches the researcher could take in conducting this social media-based research study?
3. What should the researcher be aware of from the research ethics point of view?
4. Should the researcher be concerned about issues of privacy or confidentiality in using or sharing this data?
5. What should be the role of the IRB for a study such as this?

Possible solutions and approaches (Townsend & Wallace, 2016):

1. Other than the scientific training mandated by the IRBs at the researcher's respective institution, the researcher needs to be aware of the terms and policies of the social media platform which is being used as much as possible. It is also suggested that the researcher makes the participants of the study aware of the terms and policies of the social media platform, which is being used, particularly the policies related to public data use and privacy settings.
2. As a research approach, the researcher should first find out if the "online support group" on Facebook is a "closed group" or an "open group." A "closed group" usually is a password-protected group and has a group gatekeeper. The researcher needs to inform the "gatekeeper" of the study and research plans and then decide accordingly whether to be a participant in the group or just be an observer or both (as this could bias the researcher's findings, particularly for a qualitative study).
3. From the point of view of research ethics, it's important that the researcher asks either the group gatekeeper to provide informed consent to conduct

this study; alternately the group gatekeeper may seek permission via informed consent from all the group participants in this group (this is particularly important if the researcher wishes to publish or present any or all of the collected data at scientific meetings or via scientific publications).

4. Since the information accessed in this "online support group" is sensitive, utmost care for handling "privacy" and "confidentiality" of the data needs to be taken by the researcher. The researcher may either introduce oneself to the community members or check with them if anyone would like to "opt-out" of this study. The gatekeeper can also protect some of the group members who would not like to be a part of the study by restricting researcher access to the entire group. Any data collected need to be reported in aggregate. Furthermore, care should be taken to fully anonymize data if there are fewer participants such that the data cannot be linked to a specific individual.
5. The IRB along with the Research Compliance Officer is the primary board that makes sure that the researcher is compliant with the policies of informed consent, privacy, and confidentiality such that it protects the study participants from any potential or established harm. In this case, the IRB needs to make sure that this is clearly outlined by the researcher in the proposal to the IRB. An IRB oversight is needed throughout the process of the research study (if any aspects of the research are altered) and 3 years beyond the study completion as the study output data need to be protected and saved for three years of study completion.

Case study 2: Twitter-based research study (Townsend & Wallace, 2016)

A Professor at a Southern Research University was interested in studying pro- and antivaccination narratives in light of the vaccine initiative related to the COVID-19 pandemic. It was decided that the data would be collected via Twitter—as most data on Twitter are public and hence convenient to be collected. The researcher decides to collect data over the last two weeks using hashtags #covid vaccine #vaccine refusal #vaccine benefits. Some of the early concerns about this study are that this could be considered a controversial and hence sensitive topic and the researcher could have participants who are less than 18 years of age providing comments via tweets and hence anonymity concerns arise.

Case study questions

1. Does a researcher need any kind of training to pursue such as research study?

2. What should the researcher be aware of from the research ethics point of view?
3. What should be the role of the IRB for a study such as this?

Possible solutions:

1. Other than the scientific training mandated by the IRBs at the researcher's respective institution, the researcher needs to be aware of the terms and policies of the social media platform, which is being used as much as possible. It is also suggested that the researcher makes the participants of the study aware of the terms and policies of the social media platform, which is being used, particularly the policies related to public data use and privacy settings.
2. Since the data collected for this study were via tweets using hashtags, these data could be safely considered public. In case the researcher wanted to collect data via direct communications between participants, then that was "private data" and needed much more safety precautions, particularly since this could be considered sensitive data as well. There are concerns related to "privacy" and "confidentiality" in this case as well. Since we do not know the age of the tweet contributors (as they could be underaged and hence need protection from harm), it is important that the researcher provides a paraphrased version of the participant comments rather than direct quotes (as the actual participant quotes could be linked to their user profiles and a cause of harm). In case the researcher decides to use "direct quotes" then, informed consent from those participants needs to be taken. A research output should be in terms of emerging themes that are paraphrased, and Twitter handles removed.
3. The IRB along with the Research Compliance Officer is the primary board that makes sure that the researcher is compliant with the policies of informed consent, privacy, and confidentiality such that it protects the study participants from any potential or established harm. It is also expected that the IRB has its own policies for social media data usage and research conductance to facilitate the researchers' approach and conductance of the study. The IRB needs to make sure that this is clearly outlined by the researcher in the proposal to the IRB. An IRB oversight is needed throughout the process of the research study (if any aspects of the research are altered) and three years beyond the study completion as the study output data need to be protected and saved for three years beyond study completion.

Role of confidentiality in social media usage

Confidentiality is private information that is entrusted with confidence (Confidentiality, n.d.). From a researcher's perspective and often explained by

the IRBs, "confidentiality" is when the researcher knows participants, irrespective of whether one can link a person to a set of answers. However, researchers do not present research results that identify participants. If the participant pool is small, it may be impossible to ensure confidentiality even if data are presented in the aggregate (University of Arkansas at Little Rock, n.d). Hence, confidentiality is maintained in any kind of research by reporting data in aggregate and it is challenging to maintain with a small pool of participants.

In the meantime, there are several questions to consider in "social media-based research": Will the data from the social media applications (apps) such as Facebook and Twitter be identifiable? What is the social media app's privacy policy? Does the app have access to research data? Do participants need to be trained on the use of social media apps? Do users know how to adjust security settings on their devices and apps? Should data in transit from the social media app to the researchers be encrypted? (University of Nevada Reno, 2021).

Data confidentiality is important in maintaining and transferring any data accessed using technology such as social media applications or social media platforms. Data confidentiality can be primarily maintained during the data collection phase as well as the data storage phase. In a data collection phase, researchers can ask social media users such as Facebook or Twitter to create their own "screen names" which could be possibly less identifiable. For instance, it can be linked to participant identities in a single database when downloaded. If the researcher has the participants involved in sharing opinions or other artifacts in a social media-based group, it is important to remind the research participants not to share personally identifiable information. It is recommended that the investigators send repeated announcements in a group-based social media study (Bull, 2011).

As an illustration, patients commenting on medical information on a Facebook page or sharing pictures of themselves where pictures of doctors or nurses are "tagged" can inadvertently transcend the boundaries of maintaining confidentiality. Similarly, a medical professional cannot share the private and protected medical information about a patient (which is considered confidential) via Facebook page comments although the patient himself/herself could do it based on the privacy setting set by the person on the social media platform (Medical Protection Society, n.d.). The above scenario highlights a very important aspect of the doctor-patient relationship and how social media-based platforms could jeopardize those if either party is not very cognizant of this.

Another profession where confidentiality is of paramount importance is the law. Lawyers and their clients need to make sure that no breach of confidentiality exists in the case. Because of this, case details should not inadvertently be disclosed via social media platforms or alternately used by a third party through accessing the social media pages of a client leading to unintended disclosure (Medical Protection Society, n.d.). Guidelines need to be established prior to

professionals engaging with their clients on the handling of case-based information if shared via social media platforms.

Similarly, nursing professionals who craft professional messages or share videos or pictures via social media-based platforms need to be cognizant of the HIPAA guidelines. Hence, they ought to be careful when selecting social media-based platforms for their professional consultations and/or sharing professional messages. Precaution should be taken not to violate patient or client confidentiality. In addition, crafted messages should not contradict the mission or philosophy of the organizations they represent (Bradley University, n.d.).

Review of literature

Major ethical issues related to social media

Privacy

Data privacy is one of the major issues related to social media. Ethical issues associated with social media are basically divided into individual morality and information management (Turculet, 2014). Primarily, data privacy is dependent on the individual social media platform and individual settings or preferences (Hunter et al., 2018). Interactions on social media have often been an issue not only for the public but also for individuals. For instance, despite Facebook allowing users to post their personal or private details, it has been accused of infringing individual privacy. Specifically, allegations include sharing or selling members' information with other agencies or allowing other users to share personal information. Notwithstanding, individual postings have sometimes been pulled out for contravening Facebook community standards.

Likewise, among ethical issues related to privacy is the privacy document signed by social media platform users. More often, the policy is available on social media platforms, but many users rarely take the time to read and decide the level of privacy they need. For example, Facebook has a privacy policy that allows users to decide whether they want their profile and followers to be public, or only accessible to their friends, your friends' friends, or private. However, studies show that some users are either technologically limited or unable to comprehend the language used (Turculet, 2014). As a result, it may violate ethical issues since many users end up not setting up a privacy platform. To that effect, Facebook has been accused of sharing personal information with users. Despite the challenges, researchers have suggested several measures to enhance privacy: educating users with regard to personal privacy and social media privacy policy settings; development and use of programs that detect third-party users when browsing; and users' anonymity such as lack of personal image or data (Turculet, 2014).

Confidentiality

One of the key ethical requirements of IRBs is the protection and maintenance of participants' anonymity when using social media to conduct research. Even though researchers are required to exclude items asking for personal information, individual relational links can still be used to predict the personal attributes of the users (Zimmer, 2010). Even though it can be argued that whatever information individuals post is personal profiles, social media data such as personal pictures can still be used to erode confidentiality. In addition, personal information such as profile pictures of participants might as well result in researcher biases.

Can ethics and confidentiality Coexist?

The answer to this question is yes, but with conditions. IRBs are not only required to put measures in place but must also ensure that both ethics and confidentiality are implemented. American Speech-Language-Hearing Association (ASHA, 2022), there are several measures that IRBs can implement to support both ethics and confidentiality:

- Disseminate research findings without disclosing personal identifying information.
- Secure storage of research data.
- Anonymous responses.
- Removing and coding personal information.
- Obtaining electronic or written consent.

Trust

Trust is an impediment to social media. Trust tends to emerge from a lack of proper communication and a feeling of vulnerability (Turculet, 2014). Users tend to distrust social media platforms, thus making it a complex ethical issue. There are very little progress researchers can make when the participants lack trust. It is not only difficult to recruit participants, but it is also unethical to talk them into participating in a study when they lack trust. Ideally, individuals build trust from long-term interaction with other people (Turculet, 2014). However, with social media platforms, there is no face-to-face or personal interactions. As a result of social media platforms, many participants might not be willing to engage in online studies. In addition, false information and conspiracy theories have also contributed to mistrust witnessed when using social media. As observed earlier, trust emerges spontaneously through experience and mechanisms put in place to assure users that the platform is safe.

Application of privacy and confidentiality in public health studies using social media

Even though social media has become an integral part of public health studies, it has also been compounded with issues related to privacy and confidentiality. This part of the book chapter specifically explores privacy and confidentiality issues in social media use in public health.

Despite dynamic changes in social media use, public health researchers have an obligation to ensure that they observe ethical issues related to privacy. Protecting the privacy of research participants is very important. Researchers can maximize privacy by ensuring that they grasp the default settings as well as understand whatever the users have signed for (Hunter et al., 2018). Researchers can go a step further and take advantage of social media platforms and amend privacy risks. In such incidents, utmost confidentiality should be observed. Notwithstanding, some data are general or accessible in the public domain and hence require minimal levels of confidentiality. Public health researchers have successfully used social media for contact tracing and disease surveillance. Even though this information is important to the public, confidentiality must be adhered to, so as to give users confidence. For instance, when using Facebook, researchers can adjust the settings to hide personal information such as pictures. As observed earlier, most social media platforms have attempted to put measures in place to protect users. However, it is important for researchers to familiarize themselves with confidentiality information on each platform and reconcile with the ethical requirements guiding their research. In this case, a researcher would be in a position to determine which features to hide or remove.

Second, the users should be made aware of what they are signing. It has been reported that most social media policies and guidelines are so complex that users get confused. They require a detailed approach and frequent updates for them to be well utilized by the users. Thus, it is the responsibility of researchers to ensure that they provide adequate information to the users to be aware of issues associated with their privacy and confidentiality. A study exploring COVID-9 contact tracing on Twitter found that users are likely to share their personal information if they are aware of the intended use as well as have confidence that the information will be protected (Bhatt et al., 2022). To that extent, the researchers ought to explain all the small details about confidentiality and explain to the users why they are collecting the data.

Third, researchers should only collect information that is necessary and applicable in the final analysis (Nicholas et al., 2020). Questionnaires for research questions ought to be designed in a way to capture the key research questions or hypotheses and avoid gathering any data that are not required in the study. For example, researchers can leave out sensitive information such as usernames and public identifiers. But, if for any reason personal data are collected, then it should only be accessible to the main researcher. Another approach is saving personal information separate from the rest of the data. In

other words, it should be made difficult to pair the data collected with the participant or user. In the unlikely event that there is a breach or accessibility to data, it will be impossible to compromise the personal information of the users.

In an event that a researcher uses direct quotes from social media platforms, it is recommended that the information be de-identified for the second time (Nicholas, 2020). For instance, a researcher can remove information that directly identifies the user such as the name, social media platform name, or pictures.

In the recent past, public health organizations and agencies have increased the use of electronic and social media platforms to conduct research, store information, and even submit information to coresearchers. However, these platforms, if not handled carefully, can compromise confidentiality by exposing the data to unauthorized users. To that extent, putting measures that secure and uphold confidentiality is an equally important part of the research process. The question that arises is how to balance individual and societal interests, especially when faced with an epidemic such as COVID-19. In an ideal situation, researchers are expected to assess the sensitivity of data, the possibility of maintaining confidentiality, and the risks associated with sharing or not sharing personal information (Harris, 2008). For example, sensitive data about a particular organization collected from employees might put them at risk. Such a situation demands that the information or data collected be kept in confidence. Remember, it is imperative for the users to be confident that the information they are sharing with the researcher is protected and will not expose them to undue risks.

One of the remedies is for public health researchers to establish routine disclosure protocols. This would include the appropriateness of disclosure, the integrity of the information being disclosed, the identity of the person receiving the information, and the security of the mode of data transmission (Myers et al., 2008). Education is another measure that should be incorporated into public health research. Even though there has been an outcry with regard to hacking, the real problem lies with the way the data are handled and secured by the researchers. There should be more training, increased surveillance, and accountability for data storage (Myers et al., 2008). In other words, all the persons involved in research should undergo frequent training and refresher courses. With the emergence of new social media platforms accompanied by dynamic changes, researchers have to be on top.

In order that public health experts to promote health behavior changes among patients, they have been encouraged to use social media. Nevertheless, this has led to the issue of confidentiality. Some scientists posit that social media be used for public conversations with regard to general public health issues rather than discussing individual patients (Crotty & Mostaghimi, 2014). Specifically, the patients or participants should be informed that the social media platform is not meant for clinical communication. Public conversations focus on general issues,

for example, physical violence in the local community. Participants might discuss probable causes, without pinpointing suspects within the community.

In summary, social media platforms are very useful in public health research. The increased accessibility and use of social media platforms make it logical for researchers to utilize these platforms. At the same time, measures should be put in place to ensure that the user's privacy and confidentiality are implemented. Researchers should undertake training relevant to specific platforms to avoid issues emerging from breaches of ethical principles related to research.

Chapter summary

In summary, the use and applications of social media-based platforms have been common in current times for personal as well as professional usage. Since some of the social media-based platforms such as Facebook, Twitter, and LinkedIn can be used for personal as well as professional usage, they have blurred the lines between public versus private use of these platforms for sharing content, making comments, and taking part in conversations, and attending events and chats. This chapter has addressed the use and application of social media platforms from a lens of ethics, privacy, and confidentiality.

The authors have discussed tenets of beneficence, nonmaleficence, justice, and respect for persons while considering the use and application of social media-based platforms. Furthermore, detailed discussions about the public versus private mode of operationalization of platforms such as Facebook, Twitter, and YouTube are discussed. The information gleaned from this discussion can be applied not only for personal usage of these platforms but also for professional usage by faculty, staff, researchers, and allied professionals in the fields of health care, public health, and health education. The case vignettes are specifically designed to demonstrate the emerging issues when these platforms are used in conducting a research-based study.

Finally, the chapter wouldn't be complete without a brief literature review on issues of privacy, confidentiality, and trust in the usage and application of social media platforms. Additionally, the authors also throw some light on the relevant current literature which demonstrates the use and application of social media-based platforms in health education/public health.

The authors of this book expect that the review of the material in this chapter related to ethics, privacy, and confidentiality of social media usage generates a discussion among the readers and enhances their understanding of the complexity of issues when using social media for personal as well as professional usage. It is the expectation of the authors that this chapter generates a copious and enlightening discussion among the readers, including researchers, faculty, and students on generating guidelines for navigating the privacy and confidentiality aspects of social media-based platforms while designing and implementing research studies and health care interventions. It is also expected that IRBs at diverse institutions across the nation generate detailed guidelines for use of social media-based platforms while conducting research.

Questions for discussion

1. Describe the role of ethics in the use and application of social media.
2. Compare and contrast the privacy-related issues between Facebook and Twitter—two social media-based platforms.
3. Describe the role of confidentiality while using social media-based platforms.
4. Explain the role of trust in using social media-based platforms.
5. Apply a social media-based intervention addressing a public health issue.
6. Appraise the literature on the application of social media-based studies in public health/health education.

Important terms defined

Beneficence: Beneficence is defined as an act of charity, mercy, and kindness with a strong connotation of doing good to others including moral obligation (Kinsinger, 2009).

Confidentiality: The fact of private information being kept secret (Confidentiality, n.d.).

Ethics: The principles of conduct governing an individual or a group (Ethic, n.d.).

Facebook: This is an online social media and social networking service owned by American company Meta Platforms (Facebook, n.d.).

Institutional Review Board: The Institutional Review Board (IRB) is an administrative body established to protect the rights and welfare of human research subjects recruited to participate in research activities conducted under the auspices of the institution with which it is affiliated (Oregon State University, n.d.).

Justice: The maintenance or administration of what is just especially by the impartial adjustment of conflicting claims or the assignment of merited rewards or punishments (Justice, n.d.).

Media: A medium of cultivation, conveyance, or expression (Media, n.d.).

Nonmaleficence: It means an intention to avoid needless harm or injury that can arise through acts of commission or omission (Ethics of International Engagement & Service Learning, 2011).

Public: Of relating to or affecting all the people or the whole area of a nation or state (Public, n.d.).

Public Health: The art and science dealing with the protection and improvement of community health by organized community effort and including preventive medicine and sanitary and social science (Public Health, n.d.).

Privacy: Freedom from unauthorized intrusion (Privacy, n.d.).

Social media: Forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos) (Social media, n.d.).

Trust: Assured reliance on the character, ability, strength, or truth of someone or something (Trust, n.d.).

Twitter: Twitter is a free social networking site where users broadcast short posts known as tweets (Hetler, 2022).

YouTube: It is an American online video sharing and social media platform headquartered in San Bruno, California (YouTube, n.d.).

Websites to explore

Centers for Disease Control and Prevention, social media tools, guidelines, and best practices

http://www.cdc.gov/socialmedia/tools/guidelines/index.html.

The purpose of this website is to share guidelines and best practices to use social media by the Centers for Disease Control and Prevention. Please explore this website. Read the Facebook and Twitter Guide. What did you learn about the privacy and confidentiality policy? Review the Social Media Toolkit. Can you think of an application of this tool kit in designing at least two social media based public health campaigns? How would you evaluate this campaign?

Ethical dilemmas of social media and how to navigate them from Norwegian Business School

https://www.bi.edu/research/business-review/articles/2020/07/ethical-dilemmas-of-social-media–and-how-to-navigate-them/.

The above website from a Norwegian Business School discusses ethical dilemmas in navigating social media. Do you agree with these? Do you feel these are applicable in the US context as well? Do you have any additional ideas based on this chapter about navigating these?

Internet safety rules while using social media for teens

https://arkansasag.gov/education-programs/internet-safety/

This is a website demonstrating safety rules for teens engaging in social media. Please explore this website. Did anything on this website surprise you? What do you feel is missing from these rules in terms of safety? How many of these social media applications are you familiar with?

Issues in ethics: ethical use of social media

https://www.asha.org/practice/ethics/ethical-use-of-social-media/.

This Issues in Ethics statement is new and is consistent with the Code of Ethics (2016). The Board of Ethics reviews Issues in Ethics statements periodically to ensure that they meet the needs of the professions and are consistent with the American Speech Language and Hearing Association. Compare and contrast this with the code of ethics for at least two other

organizations (e.g., National Commission for Health Education specialists, American Public Health Association, etc.) and state at least three aspects that were common and three aspects which were different.

Protecting student privacy on social media

https://www.commonsense.org/education/articles/protecting-student-privacy-on-social-media-dos-and-donts-for-teachers.

The purpose of this website is to share the do's and don'ts regarding student privacy on social media. Explore this website and read the do's and don'ts in detail. How many of these rules apply outside the school environment? Read the section on "Further reading" to enhance your understanding.

Public health guide to social media 101

https://www.rvphtc.org/wp-content/uploads/2019/05/MPHTC_SocialMediaGuide2015.pdf.

This is a Public Health Social Media training guide developed by Michigan Public Health Training Center. Please review this guide. Can you mention at least three ways in which public health professionals can benefit from this guide?

Social media research: public health versus privacy

https://www.ethicscenter.net/exploring-convergence-social-media-big-data-ethics/.

The above website and the associated video by Tim K. Mackey, MAS, PhD., Director, Global Health Policy Institute (www.ghpolicy.org) Associate Director, Joint Master's Program in Health Policy and Law & Associate Professor, UC San Diego, School of Medicine discuss ethical challenges for prescription drug abuse prevention in the social media environment. Please watch this video. Do you agree with the speaker's thoughts and points? If not, why? Are these points applicable for any other health behavior other than prescription drug abuse?

Social media and web 2.0 policy: US Department of Commerce

https://www.commerce.gov/about/policies/social-media.

This website presents a social media policy by the US Department of Commerce. Review this policy. Can you identify any strengths and weaknesses in this policy? Do you feel it's missing anything which needs to be added to it?

Theme issue: social media, ethics, and COVID-19 misinformation

https://www.jmir.org/themes/1142-theme-issue-social-media-ethics-and-covid19-misinformation.

This is a themed issue. Read any three articles from the year 2022. What were the strengths and weaknesses of these articles in terms of discussing privacy and ethical issues and their applications?

References

American Speech-Language-Hearing Association [ASHA]. (2022). https://www.asha.org/practice/ethics/confidentiality/.

Bensley, R. J., & Brookins-Fisher, J. (2019). *Community and public health education methods: A practical guide* (4th ed.). Jones and Bartlett Learning.

Bhatt, P., Vemprala, N., Valecha, R., Hariharan, G., & Rao, H. R. (2022). User privacy, surveillance and public health during COVID-19—An Examination of Twitter verse. *Information Systems Frontiers*, 1—16.

Bradley University. (n.d.) Pros and cons of social media for nursing professionals. https://onlinedegrees.bradley.edu/blog/social-media-in-nursing/.

Bull, S. (2011). *Technology-based health promotion*. Sage Publications Inc.

Buraphadeja, V., & Prabhu, S. (2020). Faculty's use of Facebook and implications for e-professionalism in Thailand. *Cogent Education, 7*(1). https://doi.org/10.1080/2331186X.2020.1774956

Cain, J., & Romanelli, F. (2009). E-professionalism: A new paradigm for a digital age. *Currents in Pharmacy Teaching and Learning, 1*(2), 66—70. https://doi.org/10.1016/j.cptl.2009.10.001

Confidentiality.(n.d.). Cambridge dictionary. Retrieved September 30th 2022 from https://dictionary.cambridge.org/us/dictionary/english/confidentiality.

Cottrell, R. R., Seabert, D. M., Spear, C. E., & McKenzie, J. F. (2023). *Principles of health education and promotion* (8th ed). Jones & Bartlett Learning.

Crotty, B. H., & Mostaghimi, A. (2014). Confidentiality in the digital age. *BMJ, 348*.

Dennen, V. P., & Burner, K. J. (2017). Identity, context collapse, and Facebook use in higher education: Putting presence and privacy at odds. *Distance Education, 38*(2), 173—192.

Ethic. (n.d.). Meriam-webster. Retreived February 27, 2023 from https://www.merriam-webster.com/dictionary/ethic#note-1.

Ethics of International Engagement and Service Learning. (2011). *Non-maleficence and beneficence*. http://ethicsofisl.ubc.ca/?page_id=172.

Facebook Help Center. (n.d.). What is public information on Facebook. https://m.facebook.com/help/203805466323736?ref=dp&_rdr.

Facebook (n.d.). Wikipedia. https://en.wikipedia.org/wiki/Facebook.

Fileborn, B. (2017). Justice 2.0: Street harassment victims' use of social media and online activism as sites of informal justice. *British Journal of Criminology, 57*, 1482—1501.

Forbes, D. (2017). Professional online presence and learning networks: Educating for ethical use of social media. *International Review of Research in Open and Distributed Learning, 18*(7), 175—190.

Fruhlinger, J. (2021). *COPPA explained: How this law protects children's privacy.* https://www.csoonline.com/article/3605113/coppa-explained-how-this-law-protects-childrens-privacy.html.

Harris, J. K. (2008). Consent and confidentiality: Exploring ethical issues in public health social network research. *Connections, 28*(2), 81—96.

Hetler, A. (2022). *Twitter. What is*. https://www.techtarget.com/whatis/definition/Twitter.

Hunter, R. F., Gough, A., O'Kane, N., McKeown, G., Fitzpatrick, A., Walker, T., & Kee, F. (2018). Ethical issues in social media research for public health. *American Journal of Public Health, 108*(3), 343—348.

Justice. (n.d.). Merriam-webster. https://www.merriam-webster.com/dictionary/justice.

Kanekar, A., & Thombre, A. (2019). *Fake medical news: Avoiding pitfalls and perils*. Family Medicine & Community Health. https://doi.org/10.1136/fmch-2019-000142

Karlis, N. (2019). *You just deleted Facebook. can you trust Facebook to delete your data?*. Salon website https://www.salon.com/2019/02/10/you-just-deleted-facebook-can-you-trust-facebook-to-delete-your-data/.

Kinsinger, F. S. (2009). Beneficence and the professional's moral imperative. *Journal of Chiropractic Humanities, 16*, 44–46.

Media(n.d.) Merriam-Webster. Retreived February 27, 2023 from https://www.merriam-webster.com/dictionary/media.

Medical Protection Society. (n.d.) Casebook. Aspects of confidentiality: social media. https://www.medicalprotection.org/southafrica/casebook/casebook-may-2014/aspects-of-confidentiality-social-media.

Meta Privacy Center. (2022). Privacy policy: What is the privacy policy and what does it cover?. https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0.

Moral. (n.d.) Merriam-Webster. https://www.merriam-webster.com/dictionary/moral.

Myers, J., Frieden, T. R., Bherwani, K. M., & Henning, K. J. (2008). Ethics in public health research: Privacy and public health at risk: Public health confidentiality in the digital age. *American Journal of Public Health, 98*(5), 793–801.

Nicholas, J., Onie, S., & Larsen, M. E. (2020). Ethics and privacy in social media research for mental health. *Current Psychiatry Reports, 22*(12), 1–7.

Office for Human Research Protections. (2021). Review of third -party research risk: Is there a role for IRBs https://www.hhs.gov/sites/default/files/2021-oew-summary-report.pdf.

Oregon State University. What is the Institutional Review Board (IRB)? https://research.oregonstate.edu/irb/frequently-asked-questions/what-institutional-review-board-irb.

Privacy. (n.d.). Merriam-webster. https://www.merriam-webster.com/dictionary/privacy.

Public Health. (n.d.). Merriam-webster. https://www.merriam-webster.com/dictionary/public%20health.

Public. (n.d.). Merriam-webster. https://www.merriam-webster.com/dictionary/public.

Relihan, T. (2018). *Social media advertising can boost fake news-or beat it*. https://mitsloan.mit.edu/ideas-made-to-matter/social-media-advertising-can-boost-fake-news-or-beat-it.

Social (n.d.) Merriam-webster. https://www.merriam-webster.com/dictionary/social.

Social media (n.d.). Merriam-webster. https://www.merriam-webster.com/dictionary/social%20media.

Townsend, L., & Wallace, C. (2016). *Social media research: A guide to ethics*. Economic and Social Research Council and the University of Aberdeen.

Tseng, T., Kanekar, A., Vogelzang, J. L., Hiller, M. D., & Headley, S. A. (2019). Commentary: Social media and the ethical principles of its use in public health and health education research. *American Journal of Health Studies, 34*(3), 155–161.

Turculet, M. (2014). Ethical issues concerning online social networks. *Procedia-Social and Behavioral Sciences, 149*, 967–972.

Twitter. (2022). *Twitter privacy policy*. https://twitter.com/en/privacy.

UA Little Rock Research Protection Program Policies and Procedures. (2018). *Office of research compliance institutional review board*. https://ualr.edu/irb/home/guidelines-and-regualtions/.

University of Arkansas at Little Rock. (n.d.). IRB Faq's https://ualr.edu/irb/home/irb-faqs/.

University of Nevada Reno. (2021). *Research integrity 410. maintaining data confidentiality*. https://www.unr.edu/research-integrity/human-research/human-research-protection-policy-manual/410-maintaining-data-confidentiality.

U.S. Department of Health and Human Services. (2021). *45 CFR 46. Office for human research protection*. https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html.

Vriens, E., & Van Ingen, E. (2018). Does the rise of the internet bring erosion of strong ties? analyses of social media use and changes in core discussion networks. *News Media & Society, 20*(7), 2432–2449.

YouTube. (n.d.) Wikipedia. https://en.wikipedia.org/wiki/YouTube.

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

Trust (n.d.) Merriam-Webster. https://www.merriam-webster.com/dictionary/trust.

Further reading

Al-Bahrani, A., Patel, D., & Sheridan, B. J. (2017). Have economic educators embraced social media as a teaching tool? *Journal of Economic Education, 48*(1), 45–50.