Social Media and Privacy

Xinru Page[*], Sara Berrios[*], Daricia Wilkinson[+], Pamela J. Wisniewski[^]

Brigham Young University, Department of Computer Science[*]

Provo, UT USA 84602

xinru@cs.byu.edu, berrios@byu.edu

Clemson University, Department of Computer Science[+]

Clemson, SC USA

dariciw@g.clemson.edu

University of Central Florida, Department of Computer Science[^]

Orlando, FL USA 32816

pamwis@ucf.edu

Abstract.

With the popularity of social media, researchers and designers must consider a wide variety of privacy concerns while optimizing for meaningful social interactions and connection. While much of the privacy literature has focused on information disclosures, the interpersonal dynamics associated with being on social media make it important for us to look beyond informational privacy concerns to view privacy as a form of interpersonal boundary regulation. In other words, attaining the right level of privacy on social media is a process of negotiating how much, how little, or when we desire to interact with others, as well as the types of information we choose to share with them or allow them to share about us. We propose a framework for how researchers and practitioners can think about privacy as a form of interpersonal boundary regulation on social media by introducing five boundary types (i.e., relational, network, territorial, disclosure, and interactional) social media users manage. We conclude by providing tools for assessing privacy concerns in social media, as well as noting several challenges that must be overcome to help people to engage more fully and stay on social media.

Keywords: Social Media, Information Disclosure, Context Collapse, Impression Management, Boundary Regulation Taxonomy, Coping Mechanisms, Privacy Fit, Boundary Preservation Concern, Boundary Enhancement Expectation, Privacy Features, Relational Hindrance, Social Disenfranchisement

Introduction

The way people communicate with one another in the 21st century has evolved rapidly. In the 1990's, if someone wanted to share a "how-to" video tutorial within their social networks, the dissemination options would be limited (e.g., email, floppy disk, or possibly a writeable compact disc). Now, social media platforms, such as Tik Tok, provide professional grade video editing and sharing capabilities that give users the potential to both create and disseminate such content to thousands of viewers within a matter of minutes. As such, social media has steadily become an integral component for how people capture aspects of their physical lives and share them with others. Social media platforms have gradually altered the way many people live [103], learn [56,139], and maintain relationships with others [123].

Carr and Hayes define social media as "internet-based channels that allow users to opportunistically interact and selectively self-present, either in real time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others [25]." Social media platforms offer new avenues for expressing oneself, experiences, and emotions with broader online communities via posts, tweets, shares, likes, and reviews. People use these platforms to talk about major milestones that bring happiness (e.g., graduation, marriage, pregnancy announcements), but they also use social media as an outlet to express grief, challenges, and to cope with crises [6,7,78]. Many scholars have highlighted the host of positive outcomes from interpersonal interactions on social media including social capital, self-esteem, and personal well-being [24,45,46,72]. Likewise, researchers have also shed light on the increased concerns over unethical data collection and privacy abuses [49,138].

This chapter highlights the privacy issues that must be addressed in the context of social media and provides guidance on how to study and design for social media privacy. We first provide an overview of the history of social media and its usage. Next, we highlight common social media privacy concerns that have arisen over the years. We also point out how scholars have identified and sought to predict privacy behavior but many efforts have failed to adequately account for individual differences. By reconceptualizing privacy in social media as a boundary regulation, we can explain these gaps from previous one-size-fits-all approaches and provide tools for measuring and studying privacy violations. Finally, we conclude with a word of caution about the consequences of ignoring privacy concerns on social media.

A Brief History of Social Media

Section Highlights:

- **Social Media use has quickly increased** over the past decade and plays a key role in social, professional, and even civic realms. The rise of social media has led to **"networked individualism".**
- This enables people to access a **wider variety of specialized relationships**, making it more likely they can meet a variety of needs. It also allows people to **project their voice** to a wider audience.
- However, people have more **frequent turnover in their social networks** and it takes much more **effort to maintain social relations** and **discern (mis) information** and **intention** behind communication.

The initial popularity of social media harkened back to the historical rise of *social network sites* (SNSs). The canonical definition of SNSs is attributed to boyd and Ellison [18] who differentiate SNSs from other forms of computer-mediated communication. According to boyd and Ellison, SNS consists of 1) profiles representing users and 2) explicit connections between these profiles that can be traversed and interacted with. A social networking profile is a self-constructed digital representation of oneself and one's social relationships. The content of these profiles varies by platform from profile pictures to personal information such as interests, demographics, and contact information. Visibility also varies by platform and often users have some control over who can see their profile (e.g., everyone or "friends"). Most SNSs also provide a way to leave messages on another's profile, such as posting to someone's timeline on Facebook or sending a mention or direct message to someone on Twitter.

Public interest and research initially focused on a small subset of SNSs (e.g., Friendster [20] and MySpace [43,58,121]), but the past decade has seen the proliferation of a much broader range of social networking technologies, as well as an evolution of SNSs into what Kane et al. term *social media networks* [66]. This extended definition emphasizes the reach of social media content beyond a single platform. It acknowledges how the boundedness of SNSs has become blurred as platform functionality that was once contained in a single platform, such as "likes," are now integrated across other websites, third-parties, and mobile apps.

Over the past decade, SNSs and social media networks have quickly become embedded in many facets of personal, professional, and social life. In that time, these platforms became more commonly known as "social media." In the U.S., only 5% of adults used social media in 2005. By 2011, half of the U.S. adult population was using social media, and 72% were social users by 2019 [100]. MySpace and Facebook dominated SNS research about a decade ago, but now other social media platforms, such as YouTube, Instagram, Snapchat, Twitter, Kik, Tik Tok, and others are popular choices among social media users. The intensity of use also has drastically increased. For example, half of Facebook users logon several

times a day, and three-quarters of Facebook users are active on the platform at least daily [100]. Worldwide, Facebook alone has 1.59 billion users who use it on a daily basis, and 2.41 billion using it at least monthly [48]. About half the users of other popular platforms such as Snapchat, Instagram, Twitter, and YouTube also report visiting those sites daily. Around the world there are 4.2 billion users, who spend a cumulative 10 billion hours a day on social networking sites [142]. However, different social networking sites are dominant in different cultures. For example, the most popular social media in China, WeChat (inc. Wēixìn 微信), has 1.213 billion monthly users [142].

While SNS profiles started as a user-crafted representation of an individual user, these profiles now also often consist of information that is passively collected, aggregated, and filtered in ways that are ambiguous to the user. This passively collected information can include data accessed through other avenues (e.g., search engines, third-party apps) beyond the platform itself [3]. Many people fail to realize that their information is being stored and used elsewhere. Compared to tracking on the web, social media platforms have access to a plethora of rich data and fine-grained personally identifiable information (PII) which could be used to make inferences about users' behavior, socio-economic status, and even their political leanings [16]. While online tracking might be valuable for social media companies to better understand how to target their consumers and personalize social media features to users' preferences, the lack of transparency regarding what and how data is collected has in more recent years lead to heightened privacy concerns and skepticism around how social media platforms are using personal data [13,39,122]. This has, in turn, contributed to a loss of trust, changes in how people interact (or not) on social media, led some users to abandon certain platforms altogether [13,38] or to seek alternative social media platforms that are more privacy-focused.

For example, WhatsApp, a popular messaging app, updated its privacy policy to allow its parent company, Facebook, and its subsidiaries to collect WhatsApp data [33]. Users were given the option to accept the terms or lose access to the app. Shortly after, WhatsApp rival Signal reported 7.5 million installs globally over four days. Recent and multiple social media data breaches have heightened people's awareness around potential inferences that could be made about them and the danger in sensitive privacy breaches. Considering the invasive nature of such practices, both consumers and companies are increasingly acknowledging the importance of privacy, control, and transparency in social media [130]. Similarly, as researchers and practitioners, we must acknowledge the importance of privacy on social media and design for the complex challenges associated with networked privacy. These types of intrusions and data privacy issues are akin to the informational privacy issues that have been investigated in context of e-commerce, websites, and online tracking (See chapters XX).

While early research into social media and privacy largely focused on these types of concerns, researchers have uncovered how the social dynamics surrounding social media have led to a broader array of social privacy issues that shape people's adoption of platforms and their usage behaviors. Rainie and Wellman explain how

the rise of social technologies, combined with ubiquitous internet and mobile access, has led to the rise of "networked individualism" [104]. People have access to a wider variety of relationships than they previously did offline in a geographically and time-bound world. These new opportunities make it more likely that people can foster relationships that meet their individual needs for havens (support and belonging), bandages (coping), safety nets (protect from crisis), and social capital (ability to survive and thrive through situation changes). Additionally, social media users can project their voice to an extended audience, including many weak ties (e.g., acquaintances and strangers). This enables individuals to meet their social, emotional, and economic needs by drawing on a myriad of specialized relationships (different individuals each particularly knowledgeable in a specific domain such as economics, politics, sports, caretaking). In this way, individuals are increasingly networked or embedded within multiple communities that serve their interests and needs.

Inversely, networked individualism has also made people less likely to have a single "home" community, dealing with more frequent turnover and change in their social networks. Rainie and Wellman describe how people's social routines are different from previous generations that were more geographically-bound – today only 10% of people's significant ties are their neighbors [104]. As such, researchers have questioned and studied the extent to which people can meaningfully maintain interpersonal relationships on social media. The upper limit for doing so has been estimated at 150 connections or "friends," [42] but social media connections often well exceed this number. With such large networks, it also takes users much more effort to distinguish (mis)information, when communication is intended for the user, and the intent behind that communication. The technical affordances of social media can also help or hinder their (in)ability to capture the nuances of the various relationships in their social network. On many social media platforms, relationships are flattened into friends and followers, making them homogenous and lacking differentiation between, for instance, casual acquaintance and trusted confidant [20,25]. These characteristics of social media lead to a host of social privacy issues which are crucial to address. In the next section, we summarize some of the key privacy challenges that arise due to the unique characteristics of social media.

Privacy Challenges in Social Media

Section Highlights:

- **Information Disclosure** privacy issues have been a dominant focus in online technologies and the primary focus for social media. It focuses on **access to data** and defining **public vs. private disclosures**. It emphasizes user control over who sees what.

- With so many people from different social circles able to access a user's social media content, the issues of **context collapse** occur. Users may post to an **imagined audience** rather than realizing that people from multiple social contexts are privy to the same information.
- The issues of **self-presentation** jump to the foreground in social media. Being able to manage impressions is a part of privacy management.
- The social nature of social media also introduces the issues of **controlling access to oneself**, both in terms of **availability** and **physical** access.
- Despite all of these privacy concerns, there is a noted **Privacy Paradox** between what people say they are concerned about, and their resulting behaviors online.

Early focus of social media privacy research was focused on helping individuals meet their privacy needs in light of four key challenges: 1) Information Disclosure, 2) Context Collapse, 3) Reputation Management, and 4) Access to Oneself. This section gives an overview of these privacy challenges and how research sought to overcome them. The remainder of this chapter shows how the research has moved beyond focusing on the individual when it comes to social media and privacy; rather, social media privacy has been reconceptualized as a dynamic process of interpersonal boundary regulation between individuals and groups.

Information Disclosure/Control over Who Sees What

A commonality among early social media privacy research is that the focus has been on information privacy and self-disclosure [135]. Self-disclosure is the information a person chooses to share with other people or websites, such as posting a status update on social media. Information privacy breaches occur when a website and/or person leaks private information about a user, sometimes unintentionally. Many studies have focused on informational privacy and on sharing information with, or withholding it from, the appropriate people [30,128,136] on social media. Privacy settings related to self-disclosure have also been studied in detail [1,34,47]. Generally, social media platforms help users control self-disclosure in two ways. First, is the level of granularity or type of information that one can share with others. Facebook is the most complex, allowing users to disclose and control more granular information for profile categories such as bio, website, email addresses, and at least eight other categories at the time of writing this chapter. Others have fewer information groupings, which make user profiles chunkier, and thus self-disclosure boundaries less granular. The second dimension is one's access level permissions, or with whom one can share personal information. The most popular social media platforms err on the side of sharing more information to more people by allowing users to give access to categories such as "Everyone", "All Users", or "Public". Similarly, many social media platforms give the option for access for "Friends" or "Followers" only.

Many researchers have highlighted how disclosures can be shared more widely than intended. Tufekci examined disclosure mechanisms used by college students

on MySpace and Facebook to manage the boundary between private and public. Findings suggest that students are more likely to adjust profile visibility rather than limiting their disclosures [143]. Other research points out how users may not want their posts to remain online indefinitely, but most social media platforms default to keeping past posts visible unless the user specifies otherwise [10]. Even when the platform offers ways to limit post sharing, there are often intentional and unintentional ways this content is shared that negates the users' wishes. For example, Twitter is a popular social media platform where users can choose to have their tweets available only to their followers. However, millions of private tweets have been retweeted, exposing private information to the public [84]. Even platforms like Snapchat, which make posts ephemeral by default, are susceptible to people taking screenshots of a snap and distributing through other channels. Thus, as social media companies continue to develop social media platforms, they should consider how to protect users from information disclosure and teach people to practice privacy protective habits.

Although some users adjust their privacy settings to limit information disclosures, they may be unaware of third-party sites that can still access their information. Scholars have emphasized the importance of educating users on the secondary use of their data, such as when third-party software takes information from their profiles [89]. Data surveillance continues to expand and the business model of social media corporations tend to favor getting more information about users, which makes it difficult for users that want to control their disclosure [106]. Third-party apps can also access information about social media users' connections without consent of the person whose information is being stored [117].

Unique Considerations for Managing Disclosures within Social Media

As mentioned earlier, social media can expand a person's network, but as that network expands and diversifies, users have less control over how their personal information is shared with others. Two unique privacy considerations for social media that arise from this tension are context collapse and imagined audiences, which we describe in more detail in the subsections below. For example, as Facebook has become a social gathering place for adults, one's "friends" may include family members, coworkers, colleagues, and acquaintances all in one virtual social sphere. Social media users may want to share information with these groups but are concerned about which audiences are appropriate for sharing what types of information. This is because these various social spheres that intersect on Facebook may not intersect as readily in the physical world (e.g., college buddies versus co-workers) [15]. These distinct social circles are brought together into one space due to social media. This concept is referred to as "context collapse" since a user's audience is no longer limited to one context (e.g., home, work, school) [18,83,109]. We highlight research on the phenomenon of the privacy paradox and explain how

context collapse and imagined audiences may help explain the apparent disconnect between users' stated privacy concerns and their actual privacy behavior.

Context Collapse. Nuanced differences between one's relationships are not fully represented on social media. While real life relationships are notorious for being complex, one of the biggest criticisms of social media platforms are that they often simplify relationships to a "binary" [21] or "monolithic" [22] dimension of either friend or not friend. Many platforms just have one type of relationship such as a "Friend," and all relationships are treated the same. Once a "friend" has been added to one's network, maintaining appropriate levels of social interactions in light of one's relationship context with this individual (and the many others within one's network) becomes even more problematic [19]. Since each friend may have different and, at times, mutually exclusive expectations, acting accordingly within a single space has become a challenge. As boyd points out, for instance, teenagers cannot be simultaneously cool to their friends and to their parents [19]. Due to this collapsed context of relationships within social media, acquaintances, family, friends, coworkers, and significant others all have the same level of access to a social media user once added to one's network - unless appropriately managed.

Research reveals that the way people manage context collapses varies. Working professionals might deal with context collapse by limiting posts containing personal information, creating different accounts, and avoiding friending those they worked with [126]. As another example, many adolescents manage context collapse by keeping their family members separate from their personal accounts [35]. Other mechanisms for managing context collapse include access-level permission to request friendship, denying friend requests, and unfriending. While there is limited support for manually assigning different privileges to each friend, the default is to start out the same and many users never change those defaults.

Privacy incidents resulting from mixing work and social media show the importance of why context collapse must be addressed. Context collapse has been shown to negatively affects those seeking employment [101], as well as endangering those who are employed. For example, a teacher in Massachusetts lost her job because she did not realize her Facebook posts were public to those who were not her friends; her complaints about parents of students getting her sick led to her getting fired from her job [59]. Many others have shared anecdotes about being fired after controversial Facebook and Twitter posts [8,57]. Even celebrities who live in the public eye can suffer from context collapse [32,68]. Kim Kardashian, for example, received intense criticism from internet fans when she posted a photo on social media of her daughter using a cellphone and wearing make-up while Kim was getting ready for hair and wardrobe [40]. Many online users criticized her parenting style for not limiting screen-time and Kim subsequently shared a photo of a stack of books that the kids have access to while she works.

Nevertheless, context collapse can also increase bridging social capital, which is the potential social benefit that can come through having ties to a wider audience. Context collapse enables this to occur by allowing people to increase their connections to weak ties and creating serendipitous situations by sharing with

people beyond whom one would normally share [32]. For example, job hunters may increase their chances of finding a job by using social media to network and connect with those they would not normally be associated with on a daily basis. Getting out a message or spreading the word can also be accomplished more easily. For instance, finding people to contribute to natural disaster funds can be effective on social media because multiple contexts can be easily reached from one account [116]. In addition to managing context collapse, social media users also have to anticipate whether they are sharing disclosures with their intended audiences.

Imagined Audiences. The disconnect between the real audience and the imagined audience on social media poses privacy risks. Understanding who can see what content, how, when, and where is key to deciding what content to share and under what circumstances. Yet, research has consistently demonstrated how users do not accurately anticipate who can potentially see their posts. This manifests as wrongly anticipating that a certain person can see content (when they cannot), as well as not realizing when another person can access posted content. Users have an "imagined audience" [80,81] to whom they are posting their content, but it often does not match the actual audience viewing the user's content. Social media users typically imagine that the audience for their social media posts are like-minded people, such as family or close-friends [81]. Sometimes, online users think of specific people or groups when creating content such as a daughter, coworkers, people who need cleaning tips, or even one's deceased father [81]. Despite these imagined audiences, privacy settings may be set so that many more people can see these posts (acquaintances, strangers, etc.). While users do tend to limit who sees their profile to a defined audience [76,84,115], they still tend to believe their posts are more private than they actually are [65,83].

Some users adopt privacy management strategies to counter potential mismatch in audience. Vitak identified several **privacy management tactics** users employ to disclose information to a limited audience [124]:

1. *Network-based.* Social media users decide who to friend or follow, therefore filtering their network of people. Some Facebook users avoid friending people they do not know. Others set friends' profiles to "hidden," so that they do not have to see their posts, but avoid the negative connotations associated with "unfriending."
2. *Platform-based*. Some users choose to use the social media sites' privacy settings to control who sees their posts. A common approach on Facebook is to change the setting to be "friends only," so that only a user's friends may see their posts.
3. *Content-based*. These users control their privacy by being careful about the information they post. If they knew that an employer could see their posts then they would avoid posting when they were at work.

4. *Profile-based*. A less commonly used approach is to create multiple accounts (on a single platform, or across platforms). For example, a professional, personal, and fun account.

As another example, teenagers often navigate public platforms by posting messages that parents or others would not understand their true meaning. For instance, by posting a song lyric or quote that is only recognized by specific individuals as a reference to a specific movie scene or ironic message, they therefore creatively limit their audience [83,87]. Others manage their audience by using more self-limiting privacy tactics like self-censorship [87], choosing just to not post something they were considering in the first place. These various tactics allow users to control who can see what on social media in different ways.

Reputation Management through Self-Presentation

Technology-mediated interactions have led to new ways of managing how we present ourselves to different groups of friends (e.g., using different profiles on the same platform based on the audience) [114]. Being able to control the way we come across to others can be a challenging privacy problem that social media users must learn to navigate. Features to limit audience can also help with managing self-presentation. Nonetheless, reputation or impression management is not just about avoiding posts or limiting access to content. Posting more content, such as selfies, is another approach used to control the way others perceive a user [102]. In this case, it is important to present the content that helps convey a certain image of oneself. Research has revealed that those who engage more in impression management tend to have more online friends and disclose more personal information [74]. Those who feel online disclosures could leave them vulnerable to negativity, such as individuals who identify as LGBTQ+, have also been found to put an emphasis on impression management in order to navigate their online presence [41]. However, studies still show that users have anxieties around not having control over how they are presented [118]. Social media users worry not only about what they post, but are concerned about how others' postings will reflect on them [143].

Another dimension that affects impression management attitudes is how social media platforms vary in their policies on whether user profiles must be consistent with their offline identities. Facebook's real name policy, for instance, requires that people use their real name and represent themselves as one person, corresponding to their offline identities. Research confirms that online profiles actually do reflect users' authentic personalities [11]. However, some platforms more easily facilitate identity exploration and have evolved norms encouraging it. For example, Finsta accounts popped up on Instagram a few years after the company started. These accounts are "Fake Instagram" accounts often sharing content that the user does not want to associate with their more public identity, allowing for more identity

exploration. This may have arisen from the social norm that has evolved where Instagram users often feel like they need to present an ideal self. Scholars have observed such pressure on Instagram more than on other platforms like Snapchat [28]. While the ability to craft an online image separate from one's offline identity may be more prevalent on platforms like Instagram, certain types of social media such as location-sharing social networks are deeply tied to one's offline self, sharing actual physical location of its users. Users of Foursquare, a popular location sharing app, have leveraged this tight coupling for impression management. Scholars have observed that users try to impress their friends or family members about the places they spend their time while skipping "check in" at places like McDonalds or work for fear of appearing boring or unimpressive [79].

Regardless of how tightly one's online presence corresponds with their offline identity, concerns about self-presentation can arise. For example, users may lie about their location on location-sharing platforms as an impression management tactic and have concerns about harming their relationships with others [92]. On the other hand, Finstas are meant to help with self-presentation by hiding one's true identity. Ironically, the content posted may be even more representative of the user's attitudes and activities than the idealized images on one's public-facing account. These contrasting examples illustrate how self-presentation concerns are complicated.

What further complicates reputation management is that social media content is shared and consumed by a group of people and not just individuals or dyads. Thus, self-presentation is not only controlled by the individual, but by others who might post pictures and/or tag that individual. Even when Friends/Followers do not directly post about the user, their actions can reflect on the user just by virtue of being connected with them. The issues of co-owned data and how to negotiate disclosure rules is a key area of privacy research on the rise. We refer you to Metzger and Suh (Chapter XX) who go in-depth on this topic.

Access to Oneself

A final privacy challenge many social media users encounter is controlling accessibility others have to them. Some social media platforms automatically display when someone is online, which may invite interaction whether users want to be accessible or not. Controlling access to oneself is not as straightforward as limiting or blocking certain people's access. For instance, studies have also shown that social pressures influence individuals to accept friend requests from "weak ties" as well as true friends [19,60]. As a result, the social dynamics on social media are becoming more complex, creating social anxiety and drama for many social media users [19,22,60]. Although a user may want to control who can interact with him or her, they may be worried about how using privacy features such as "blocking" other accounts may send the wrong signal to others and hurt their relationships [91]. In fact, an online social norm called "hyperfriending" [51] has developed where only

25% of a user's online connections represent true friendship [140]. This may undermine the privacy individuals wished they had over who interacts with them on their various accounts. Due to social norms or etiquette, users may feel compelled to interact with others online [111]. Even if users don't feel like they need to interact, they can sometimes get annoyed or overwhelmed by seeing too much information from others [44]. Their mental state is being bombarded by an overload of information and they may feel their attention is being captured.

Many social media sites now include location-sharing features to be able to tell people where they are by checking in to various locations, tag photos or posts, or even share location in real time. Therefore, privacy issues may also arise when sharing one's location on social media and receiving undesirable attention. Studies point out user concerns about how others may use knowledge of that location to reach out and ask to meet up, or even to physically go find the person [94]. In fact, research has found that people may not be as concerned about the private nature of disclosing location as they are concerned for disturbing others or being disturbed oneself as a result of location sharing [63]. This makes sense given that analysis of mobile phone conversations reveals that describing one's location plays a big role in signaling availability and creating social awareness [14,63]. Some scholars focus on the potential harm that may come because of sharing their location. Tsai et al. surveyed people about perceived risks and found that fear of potential stalkers is one of the biggest barriers to adopting location-sharing services [120]. Nevertheless, studies have also found that many individuals believe that the benefits of using location sharing outweigh the hypothetical costs. Foursquare users have expressed fears that strangers could use the application to stalk them [79]. These concerns may explain why users share their location more often with close relationships [128].

Geotagging is another area of privacy concern for online users. Geotagging is when media (photo, website, QR codes) contain metadata with geographical information. More often the information is longitudinal and latitudinal coordinates, but sometimes even time stamps are attached to photos people post. This poses a threat to individuals that post online without realizing that their photos can reveal sensitive information. For example, one study assessed Craiglist postings and demonstrated how they could extract location and hours a person would likely be home based on a photo the individual listed [52]. The study even pinpointed the exact home address of a celebrity TV host based on their posted Twitter photos. Researchers point out how many users are unaware that their physical safety is at risk when they post photos of themselves or indicate they are on vacation [48,52,113]. Doing so may make them easy targets for robbers or stalkers to know when and where to find them.

Privacy Paradox

While researchers have investigated these various privacy attitudes, perceptions, and behaviors, the privacy paradox (where behavior does not match with stated privacy concerns) has been especially salient on social media [9,26,53,61,98,134]. As a result, much research focuses on understanding the decision-making process behind self-disclosure [137]. Scholars that view disclosure as a result of weighing the costs and the benefits of disclosing information use the term "privacy calculus" to characterize this process [37]. Other research draws on the theory of bounded rationality to explain how people's actions are not fully rational [107]. They are often guided by heuristic cues which do not necessarily lead them to make the best privacy decisions [70]. Indeed, a large body of literature has tried to dispel or explain the privacy paradox [36,53,71].

Reconceptualizing Social Media Privacy as Boundary Regulation

Section Highlights:

- By reconceptualizing privacy in social media as a **Boundary Regulation**, we can see that the seeming paradox in privacy is actually a balance between being too open or disclosing too much, and being too inaccessible or disclosing too little. The latter can result in social isolation which is privacy regulation gone wrong.
- In context of social media, there are **five different types of privacy boundaries** that should be considered.
- People use various methods of **coping with privacy violations**, many not tied to disclosing less information.

Drawing from Altman's theories of privacy in the offline world (See Chapter XX), Palen and Dourish describe how, just like in the real world, social media privacy is a boundary regulation process along various dimensions besides just disclosure [97]. Privacy can also involve regulating interactional boundaries with friends or followers online and the level of accessibility one desires to those people. For example, if a Facebook user wants to limit the people that can post on their wall, they can exclude certain people. Research has identified other threats to interpersonal boundary regulation that arise out of the unique nature of social media [143]. First, as mentioned previously, the threat to spatial boundaries occurs because our audiences are obscured so that we no longer have a good sense of whom we may be interacting with. Second, temporal boundaries are blurred because any interaction may now occur asynchronously at some time in the future due to the virtual persistence of data. Third, multiple interpersonal spaces are merging and overlapping in a way that has caused a "steady erosion of clearly situated action [55]." Since each space may have different and, at times, mutually exclusive behavioral requirements, acting accordingly within those spaces has become more of a challenge to manage context collapses [143]. Along with these problems, a major interpersonal boundary regulation challenge is that social media

environments often take control of boundary regulation away from the end users. For instance, Facebook's popular "Timeline" automatically (based on an obscure algorithm) broadcasts an individual's content and interactions to all of his or her friends [47]. Thus, Facebook users struggle to keep up to date on how to manage interactions within these spaces as Facebook, not the end user, controls what is shared with whom.

Boundary Regulation on Social Media

One conceptualization of privacy that has become popular in the recent literature is viewing privacy on social media as a form of interpersonal boundary regulation. These scholars have characterized privacy as finding the optimal or appropriate level of privacy, rather than the act of withholding self-disclosures. That is, it is just as important to avoid over disclosing as it is to avoid under disclosing. Therefore, disclosure is considered a boundary that must be regulated so that it is not too much or too little. Petronio's Communication Privacy Management theory (CPM) emphasizes how disclosing information (See Chapter XX) is vital for building relationships, creating closeness, and creating intimacy [99]. Thus, social isolation and loneliness resulting from under disclosure can be outcomes of privacy regulation gone wrong just as much as social crowding can be an issue. Similarly, the framework of contextual integrity explains that context-relative informational norms define privacy expectations and appropriate information flows and so a disclosure in one context (such as your doctor asking you for your personal medical details) may be perfectly appropriate in that context but not in another (such as your employer asking you for your personal medical details) [86]. Here it is not just about an information disclosure boundary, but about a relationship boundary where the appropriate disclosure depends on the relationship between the discloser and the recipient.

Drawing on Altman's theory of boundary regulation, Wisniewski et al. created a useful taxonomy detailing the various types of privacy boundaries that are relevant for managing one's privacy on social media [132]. They identified five distinct privacy boundaries relevant to social media:

1. ***Relationship.*** This involves regulating who is in one's social network as well as appropriate interactions for each relationship type.
2. ***Network.*** This consists of regulating access to one's social connections as well as interactions between those connections.
3. ***Territorial.*** This has to do with regulating what content comes in for personal consumption and what is available in interactional spaces.
4. ***Disclosure.*** The literature commonly focuses on this aspect which consists of regulating what personal and co-owned information is disclosed to one's social network.

5. ***Interactional.*** This applies to regulating potential interaction with those within and outside of one's social network.

Of these boundary types, Wisniewski et al. emphasize the most important is maintaining relationship boundaries between people. Similarly, Child and Petronio note that "one of the most obvious issues emerging from the impact of social network site use is the challenge of drawing boundary lines that denote where relationships begin and end," [144]. Making sure that social media facilitates behavior appropriate to each of the user's relationships is a major challenge.

Each of these interpersonal boundaries can be further classified into regulation of more fine-grained dimensions. In table x we summarize the different ways that each of these five interpersonal boundaries can be regulated on social media:

Boundary	**Dimensions**	**Description**	**Example**
Disclosure	Self-disclosure	Regulating your own information disclosures	Limiting the audience of a post
	Confidant-disclosure	Regulating the dissemination of co-owned information	Asking family not to post pictures of your baby until you consent
Relationship	Connection	Regulating the members of your network	Adding or deleting friends
	Context	Regulating various interactions depending on the nature of the relationship	Sharing specific content with colleagues versus college friends
Network	Discovery	Controlling the access others have to your network connections	Restricting your friend list to show mutual friends only
	Intersection	Managing interactions between groups or connections	Hiding a polarizing comment from your work friend
Territorial	Inward-facing	Regulating content for consumption	Using filters for content
	Outward-facing	Controlling the creation of semi-public content	Limiting who can post on your profile/wall
Interactional	Disabling	Managing interactions through the use or non-use of platform features	Deactivating Messenger to avoid messages
	Blocking	Limiting access to specific persons	Blocking an unwanted friend

Next, we describe each of these interpersonal boundaries in more detail.

Self- and Confidant Disclosures. The information disclosure concerns described in the previous Privacy Challenges section are the focus of privacy around disclosure boundaries. Posting norms on social media platforms often encourage the disclosure

of one's personal information (e.g., age, sexual orientation, location, personal images) [29,125]**.** Disclosing such information can leave one open to financial, personal, and professional risks such as identity theft [50,106]. However, there are motivations for disclosing personal information. For example, research suggests that posting behaviors on social media platforms have a significant relationship with a desire for positive self-presentation [2,73]. Privacy management is necessary for balancing the benefits of disclosure and its associated risks. This involves regulating both *self-disclosure* for information about one's self and *confidant-disclosure* boundaries for information that is "co-owned" with others [99] (e.g., a photograph that includes other people, or information about oneself that is shared with another in confidence).

There are a variety of disclosure boundary regulation mechanisms on social media interfaces. Many platforms offer users the freedom to selectively share various types of information, create personal biographies, share links to their websites, or post their birthday. Self-disclosure can also be maintained through privacy settings such as granular control over who has access to specific posts. The level of information one wishes to disclose could be managed by various privacy settings. Many social media platforms encourage multi-party participation with features such as tagging, sub-tweeting, or replying to others' posts. This level of engagement promotes the celebration of shared moments or co-owned information/content. At the same time, it increases possibilities for breaching confidentiality and can create unwanted situations such as posting congratulations to a pregnancy that has not yet been announced to most family members or friends. Some ways that people manage violations of disclosure boundaries are to reactively confront the violator in private, or to stop using the platform after the unexpected disclosure [119].

Relationship Connection and Context. Relationship boundaries have to do with who the user accepts into his or her "friend group" and consequently shapes the nature of online interactions within a person's social network. Social media platforms have embedded the idea of "friend-based privacy" where information and interactional access is primarily dependent on one's connections. The structure of one's network can affect the level of engagement and the types of disclosures made on a platform. Individuals with more open relationship boundaries may have higher instances of weak ties compared to others who may employ stricter rules for including people into their inner circles. For example, studies have found people who engage in "hyper-adding", namely adding a significant number of persons to their network which could result in a higher distribution of "weak ties" [19,51].

After users accept friends and make connections, they must manage overlapping contexts such as work, family, or acquaintances. This leads to the types of privacy

issues discussed under Context Collapse in the previous Privacy Challenges section. Research shows that boundary violations are hardly remedied by blocking or unfriending unless in extreme cases [131]. Furthermore, users rarely organize their friends into groups (and some social media platforms do not offer that functionality) [119]. People are either unaware of the feature, think it takes too much time, or are concerned that the wrong person would still see their information. As a result, users often feel they have to sacrifice being authentic online to control their privacy.

Network Discovery and Interaction. An individual's social media network is often public knowledge and there are advantages and disadvantages of having friends being aware of one's social connections (a.k.a., friends list or followers). Network boundary mechanisms enable people to identify groups of people and manage interactions between the various groups. We highlight two types of network boundaries, namely, network discovery and network intersection boundaries. First, network discovery boundaries are primarily centered around the act of regulating the type of access others have to one's network connections. Implementing an open approach to network discovery boundaries may create problems that may arise including competition as competitors within the same industry could steal clients by carefully selecting from a publicly-facing friend list. Another issue arises when a person's friend does not have a good reputation and that connection is negatively received by others within that social group. Sometimes the result is positive, for example, when friends or family find they have mutual connections thus building social capital. Some social media platforms offer the ability to hide friend groups from everyone.

Network-intersection boundaries involve the regulation of the interactions among different friend groups within one's social network. Social media users have expressed the benefits of engaging in discourse online with people who they may not personally know offline [17]. In contrast, clashes within one's friend list due to opposing political views or personal stances could create tensions that would make moderating a post difficult. These boundaries could be harder to control and sometimes lead to conflict if one is forced to choose which friends can participate in discussions.

Inward- and Outward-Facing Territories. Territorial boundaries include "places and objects in the environment" to indicate "ownership, possession, and occasional active defense" [4]. Within social media, there are features that are either inward-facing territories or outward-facing territories. Inward-facing territory are commonly characterized as spaces where users could find updates on their friends and see the content their connections were posting (such as the "news feed" on Facebook or "updates" on LinkedIn). To control their inward-facing territories,

individuals could hide posts from specific people, adjust their privacy settings, and use filters to find specific information.

These territories are constantly being updated with photos, videos, news articles that are personalized and not public facing which contributes to an overall low priority for territorial management [119]. Most choose to ignore content that is irrelevant to them rather than employing privacy features. In addition, once privacy features are used to hide content from particular friends, users rarely revisit that decision to reconsider including content within that territory from that person.

It is important to note that the key characteristic of outward-facing territory management is the regulation of potentially unsatisfactory interactions rather than a fear of information exposure. One example of an outward-facing territory is Facebook's wall/timeline, where a person's friend may contribute to your social media presence. Outward-facing territories fall between a public and private place, which creates more risk of unintended boundary violations. Altman argues that "because of their semipublic quality [outward-facing territories] often have unclear rules regarding their use and are susceptible to encroachment by a variety of users, sometimes inappropriately and sometimes predisposing to social conflict" [4]. Similar to confidant-disclosure described above, connections may post (unwanted) content on a user's wall that could lead to turbulence if that content is later deleted.

Interactional Disabling and Blocking. Interactional boundaries limit the need for other boundary regulations discussed because a person reduces access to oneself by disabling features [119]. For example, a user may deactivate Facebook messenger to avoid receiving messages but reactivate the app when they deem that interaction to be welcomed. In a similar regard, disabling semi-public features of the interface (such as the wall on Facebook) could assist users in having a greater sense of control. This manifestation of interaction withdrawal is typically not directed at reducing interaction with a specific person, rather, it may be motivated by a high desire to control one's online spaces. As such, disabling features are associated with perceptions of mistrust within one's network and a desire to limit interruptions [131]. On the more extreme end, blocking could also be employed to regulate interactional boundaries. Unlike other withdrawal mechanisms such as disabling your wall, picture tagging, or chat, blocking is inherently targeted. The act represents the rejection and revocation of access to oneself from a particular party. Some social media platforms allow users to block other people or pages, meaning that the blocked person may not contact or interact with the user in any form. Generally, blocking a person results from a negative experience such as stalking or being bombarded with unwanted content [88].

Coping with Social Media Privacy Violations

Overtime, many social media platforms have implemented new privacy features that attempt to address evolving privacy risks and users' need for more granular control online. While this effort is commendable, Ellison et al. argue that "privacy behaviors on social networking sites are not limited to privacy settings" [47]. Thus, social media users still venture outside the realm of privacy settings to achieve appropriate levels of social interactions. Coping mechanisms can be viewed as behaviors utilized to maintain or regain interpersonal boundaries [132]. Although these coping approaches may often be sub-optimal, Wisniewski et al.'s framework of coping strategies for maintaining one's privacy provide insight into the struggles many social media users face in maintaining these boundaries.

Filtering. This approach is often defined as the "reduction of intensity of inputs" [4]. Filtering includes selecting whom one will accept into their online social circle and is often used in the management of relational boundaries. Filtering techniques may include relying on social cues (e.g., viewing the profile picture or examining mutual friends) before confirming the addition of a new connection. Other methods leverage non-privacy related features that are repurposed to manage interactions based on relation context. For example, creating multiple accounts on the same platform to separate professional connections from personal friends.

Ignoring. The vast amount of information on social media could easily become overwhelming and difficult to consume. Therefore, social media users may opt to ignore posts or skim through information to decide which ones should receive priority for engagement. Ignoring is most common for inward-facing territories such as your "Feed" page. The over reliance on this approach might increase the chances of missing critical moments that connections shared.

Blocking. Blocking is a more extreme approach to interactional boundary management compared to filtering and ignoring, which contributes to lower levels of reported usage [67]. As an alternative, users have developed other technology-supported mechanisms that would allow them to avoid unwanted interactions. As an example, Wisniewski et al. describes using pseudonyms on Facebook to make it more difficult to find a user on the platform [132]. Another method for blocking unwanted interactions is to use the account of a close friend or loved one to enjoy the benefits of the content on the platform without the hassle of expected interactions. Page et al. highlight this type of secondary use for those who avoid social media because of social anxieties, harassment, and other social barriers [95].

Withdrawal. When some users feel they are losing control, they withdraw from social media by doing one of the following: deleting their account, censoring their posts, or avoiding confrontation. As a result, a common technique is limiting or adjusting the information shared (even avoiding posts that may be received

negatively) [110]. Das and Kramer found that "people with more boundaries to regulate censor more; people who exercise more control over their audience censor more content; and, users with more politically and age diverse friends censor less, in general" [31]. Withdrawal suggests that some users think the risks outweigh the benefits of social media.

Aggression. Unlike offensive coping mechanisms such as filtering, blocking, or withdrawal, social media users resort to more defensive mechanisms when the intention is to create interactions that may be confrontational. Aggressive behavior is displayed when the goal is to seek revenge or garner attention from specific people or groups. Some users may choose to exploit subliminal references in their posts to indirectly address or offend specific persons (e.g., an ex-partner, coworker, family member).

Compliance. Compliance is giving in to pressures (external or internal) and adjusting one's interpersonal boundary preferences for others. Altman describes this as "repeated failures to achieve a balance between achieved and desired levels of privacy" [4]. Relinquishing one's interactional privacy needs to accommodate pressures of disclosure, non-disclosure, or friending preferences could result in a perceived loss of control over social interactions.

Compromise. A healthy strategy for managing social media boundary violations is communicating with the other person involved and finding a resolution. Prior work indicates that most users that compromise do so offline [132]. These compromises are mostly with closer friends who the user can contact through email, phone call, or messaging. These more private scenarios avoid other people becoming involved online. Also, many compromises are about tagging someone in photos or sharing personal information about another user (i.e., confidant-disclosure).

In addition to this coping framework for social media privacy, Stutzman examined the creation of multiple profiles on social media websites, primarily Facebook, as an information regulation mechanism. Through grounded theory, he identified three types of information boundary regulation within this context (pseudonymity, practical obscurity, and transparent separations) and four over-arching motives for these mechanisms (privacy, identity, utility, and propriety) [114]. Lampinen et al. created a framework of strategies for managing private versus public disclosures. It defined three dimensions by which strategies differed: behavioral vs. mental, individual vs. collaborative, and preventative vs. corrective [75,114]. The various coping frameworks conceptualize privacy as a process of interpersonal boundary regulation. However, they do not solve the problem of managing privacy on these platforms. They do attempt to model the complexity of privacy management in a way that better reflects the complex nature of interpersonal relationships, rather than as a matter of withholding versus disclosing private information.

Addressing Privacy Challenges

Section Highlights:

- Rather than just measuring privacy concerns, researchers and designers should focus on understanding attitudes towards boundary regulation. Validated tools for measuring **Boundary Preservation Concern** and **Boundary Enhancement Expectations** are provided in this chapter.
- **Privacy features** need to be designed to account for **individual differences** in how they are perceived and used. While some feel features like untag, unfriend, and delete are useful, others are worried about how using such features will impact their relationships.
- Unaddressed privacy concerns can serve as a barrier to using social media. It is crucial to design for not only **functional privacy concerns** (e.g., being overloaded by information, guarding from inappropriate data access), but **social privacy concerns** as well (e.g., unwelcome interactions, pressures surrounding appropriate self-presentation).

This section describes how to better identify privacy concerns by measuring them from a boundary regulation perspective. We also emphasize the importance of individual differences when designing privacy features. Finally, we elaborate on a crucial set of social privacy issues that we feel are a priority to address. While many social media users may feel these types of social pressures to some degree, these problems have pushed some of society's most vulnerable to complete abandonment of social media despite their desire for social connection. We call on social media designers and researchers to focus on these problems which are a side effect of the technologies we have created.

Understanding People and Their Privacy Concerns

Understanding social media privacy as a boundary regulation allows us to better conceptualize people's attitudes and behaviors. It helps us anticipate their concerns and balance between too little or too much privacy. However, many existing tools for measuring privacy come from the information privacy perspective [23,82,127] and focus on data collection by organizations, errors, secondary use, or technical control of data. In detailing the various types of privacy boundaries that are relevant for managing one's privacy on social media, Wisniewski et al. [119] emphasized that the most important is maintaining relationship boundaries between people.

Page et al. [90,94] similarly found that concerns about damaging relationship boundaries are actually at the root of low-level privacy concerns such as worrying about who sees what, being too accessible, or being bothered or bothering others by sharing too much information. For instance, a typically cited privacy concern such

as being worried about a stranger knowing one's current location, turns out to be a privacy concern only if an individual expects that a stranger might violate typical relationship expectations. Their research revealed that many people were unconcerned about strangers knowing their location and explained that no one would care enough to use that information to come find them. They did not expect anyone to violate relationship boundaries and so were privacy unconcerned. On the other hand, those who felt there was a likelihood of someone using their location for nefarious purposes were privacy concerned. Social media enabling a negative change in relationship boundaries and the types of interactions that are now possible (such as strangers now being able to locate me) drives privacy concerns.

In fact, while scholars have used many lower-level privacy concerns such as being worried about sharing information to predict social media usage and adoption they have met with mixed success leading to the commonly observed privacy paradox. However, research shows that preserving one's relationship boundaries is at the root of these low-level online privacy concerns (e.g., informational, psychological, interactional, and physical privacy concerns) and is a significant predictor of social media usage [90,94]. In other words, concerns about social media damaging one's relationships (a.k.a., relationship boundary regulation) is what drives privacy concerns.

Measuring Privacy Concerns

Boundary regulation plays a key role in maintaining the right level of privacy on social media, but how do we evaluate whether a platform is adequately supporting it? A popular scale for testing users' awareness of secondary access is the Internet Users' Information Privacy Concerns (IUIPC) scale, which measures their perceptions of collection, control, and awareness of user data [82]. An important finding is that users "want to know and have control over their information stored in marketers' databases." This indicates that social media should be designed such that people know where their data goes. However, throughout this chapter it is evident that research on social media privacy has found concerns about social privacy more salient. In fact, the focus on relationship boundaries is a key privacy boundary to consider and measure in evaluating privacy concerns. Thus, having a scale to measure relationship boundary regulation would allow researchers and designers to better evaluate social media privacy.

Here we present validated relationship boundary regulation survey items developed by Page et al. which predict adoption and usage for various social media including Facebook, Twitter, LinkedIn, Instagram, and location-sharing social media [90,93]. These survey items can be used to evaluate privacy concerns for use of existing social media platforms, as well as capturing attitudes about new features or platforms. The survey items capture attitudes about one's ability to regulate relationship boundaries when using a social media platform and are administered with a 7-pt Likert scale (-3=Disagree Completely, -2=Disagree Mostly, -1 Disagree

Slightly, 0=Neither agree nor disagree, 1=Agree Slightly, 2=Agree Mostly, 3=Agree Completely). These items measure both concerns and positive expectations:

Attitude	Survey Items
Relationship Boundary Preservation Concerns (BPC)	I'm worried others will use <platform> in a way that is out of line with our relationship.
	<Platform> exposes information that will negatively affect my relationship with others.
	I'm concerned that using <platform> will trigger changes in behavior that hurt my relationships.
	It is likely that using <platform> will negatively impact my relationships with others.
Relationship Boundary Enhancement Expectation (BEE)	Using <platform> will improve my relationships with others.
	<Platform> supports new behaviors that will improve my relationships.
	Using <platform> enhances my relationships with others by keeping us better informed.
	I feel others will use <platform> in a way that pushes our relationship in a positive direction.

When evaluating a new or existing social media platform, the *Relationship Boundary Preservation Concern (BPC)* items can be used to gauge user's concerns about harming their relationships. A higher score would indicate that more support for privacy management is needed on a given platform. The *Relationship Boundary Enhancement Expectation* items *(BEE)* can also be used to evaluate whether users expect that using the platform will improve the user's relationships. A high score is important to driving adoption and usage – having low concerns alone is not enough to drive usage. Along similar lines, even if users have high concerns, they may be counteracted by a perceived high level of benefits and so users remain frequent users of a platform. For instance, Facebook, one of the most widely used platforms, was shown to both invoke high levels of concern as well as high levels of enhancement expectation [90]. However, note that high frequency of use does not necessarily mean high levels of engagement (e.g., posting, commenting) or that users don't employ suboptimal workarounds (e.g., being vague in their posts) [91]. On the other hand, Twitter has a higher level of concerns compared to perceived enhancement and, accordingly, lower levels of usage [90].

In the validation studies, the set of survey items representing BPC were treated as a scale and factor analysis used to compute a single score. Similarly, the ones representing BEE were used to generate a single factor score to represent that construct. These could be used to evaluate new features or platforms in the lab or after deployment. For instance, after performing tasks on a new feature or platform, the user can answer these questions and the designer can compare the responses

between different designs in A/B testing, or to predict usage frequency and adoption intentions (e.g., see [90,96] for detailed examples). Moreover, by correlating BPC or BEE with demographics or other customer segmentations (e.g., age, whether they are new customers, purpose for using the platform) product designers may be able to identify attitudes that are connected with certain segments of their customer base and address it directly.

Designing Privacy Features

When designing for privacy features, a crucial aspect to consider is individual differences. Privacy is not one-size-fits all: there are many variations in how people feel, what they expect, and how they behave. Because social media connects individuals with diverse needs and expectations, and from a myriad of contexts, a necessity in addressing social media privacy is understanding individual differences in privacy attitudes and behaviors. Many individual differences have been identified that shape privacy needs and preferences [18] and behaviors [3,6,37].

Scholars have established that privacy as a construct is not limited to informational privacy (i.e., understanding the flow of data) but also includes social privacy concerns that may be more interactional (e.g., accessibility), or psychological in nature (e.g., self-presentation) [50,112]. Thus, a host of attitudes and experiences could shape an individual's view on what it means to have privacy online. For example, people's preferences for privacy tools could be heavily influenced by the type of data being shared or the recipient of that data [30,69,129]. Likewise, prior experiences (negative or positive) could shape how people interact online which could affect disclosure [64]. Context and relevance have also been found to significantly influence privacy behavior online. Drawing from the Contextual Integrity framework, many researchers argue that when people perceive data collection to be reasonable or appropriate, they are more likely to share information [85]. On the other hand, research has shown that when faced with uncomfortable scenarios people employ privacy protective behaviors such as non-disclosure or falsifying information [105]. Research has also pointed to personal characteristics that could shape digital privacy behavior such as personality, culture, gender, age, and social norms [12,27,62,62,77,80,86,108].

While identifying concerns about damaging one's relationships is important to measure, understanding the individual differences that can lead someone to be concerned can provide insight into addressing these concerns. For instance, through a series of investigations, Page et al. uncovered a communication style that predicts concerns about preserving relationship boundaries on many different social media platforms [90,93,96]. This communication style is characterized by wanting to put information out there so that the individual does not need to proactively inform others. Those who prefer an FYI (For Your Information) communication style are less concerned about relationship boundary preservation and, as a result, exhibit higher levels of engagement, interactions, and use of social media than low FYI

communicators. For example, the survey items that capture an FYI communication style preference for location-sharing social media are: “I want the people I know to be aware of my location, without having to bother to tell them”, “I would prefer to make my location available to the people I know, so that they can see it whenever they need it”, and “The people I know should be able to get my location whenever they feel they need it.” Each item is administered with a 7-pt likert scale (Disagree strongly, Disagree moderately, Disagree slightly, Neutral, Agree slightly, Agree moderately, Agree strongly). For other social media platforms, the information type is adjusted (i.e., “what I’m up to” instead of “my location”).

Consequently, this raises concern over implications for non-FYI communicators since the design of major social media platforms are catered to FYI communicators [90,93]. Drawing on this insight, Page demonstrated how considering the user’s communication style when designing location-sharing social media interfaces can alleviate boundary preservation concerns [96]. Certain design choices such as choosing a request-based location sharing interaction can lower concerns for non-FYI communicators, while continuous location-sharing and check-in type interactions that are typical in social media may be fine for FYI communicators.

This demonstrates that researchers should consider in the design of social media individual differences that affect privacy attitudes. Another individual difference in attitudes towards privacy features is a user’s apprehension that using common features such as untag, delete, or unfriend/unfollow can act as a hindrance in their relationships with others. Page et al. identified that while many use privacy features and perceive them as a tool useful for protecting their privacy, there are also many who are concerned about how using privacy features could hurt their relationships with others (e.g., being worried about offending others by untagging or unfriending) [91]. Instead, those individuals would use alternative privacy management tactics such as vaguebooking (not sharing specific details and using vague posts). Designers need to be aware that privacy features also need to be catered to individual variations in attitudes as well or else they may be ineffective and unused by certain segments of the user population.

Privacy Concerns and Social Disenfranchisement

A significant amount of research within the domain of social media non-use has been focused on functional barriers that hinder adoption. In many cases, non-use is traced to a lack of access (e.g., limited access to technology, financial resources, or the internet). However, the push against adoption and subsequent usage can be voluntary [133] due to functional privacy concerns such as concerns about data breaches, information overload, or annoying posts [95]. Several social media companies have also implemented features such as time limits to help users counter overuse [141].

Likewise, it is equally important to consider social barriers that prevent social media engagement for people who really could use the social connection. Sharing

about distressing experiences can be beneficial and reduce stigma, improve connection and interpersonal relationships with one's network, and enhance well-being [5,6,7,54]. However, Page et al. identified a class of barriers that highlight social privacy concerns rooted in social anxiety or concerns about being overly influenced by others on social media. This is in contrast to the prior school of thought that focused primarily on functional motivations as barriers that influence non-use (see Figure x) [95]. They point out that many who are already vulnerable avoid social media due to social barriers such as online harassment or paralysis over making decisions pertaining to online social interactions. Yet, they are also the ones who could benefit greatly from social connection and who end up losing touch with friends and social support by being off social media. They term this lose-lose situation of negative social consequences that arise when using social media as well as consequences from not using it, *social disenfranchisement*. They call on designers to address such social barriers and to realize that in designing the user experience to connect users so well, they are implicitly designing the non-user experience of being left out. Given that social media usage may not always be a viable option, designers should design to alleviate the negative consequences of non-use.

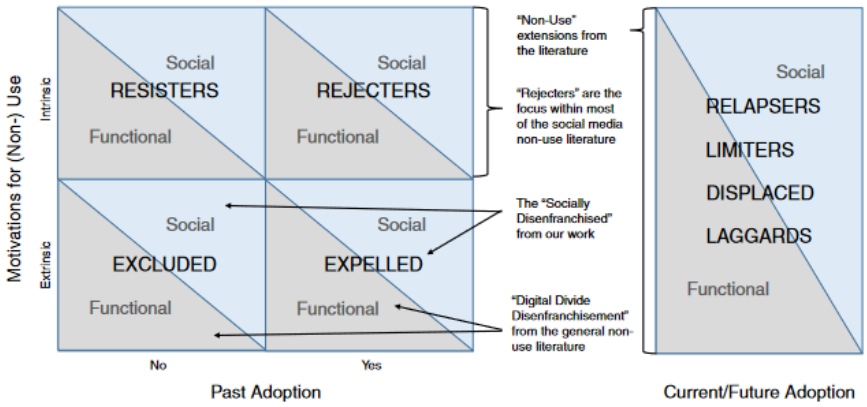

Figure 1 Extension of Wyatt's frame that divided non-users along the dimensions of whether someone has used the technology in the past, and the motivation for adoption (Extrinsic, e.g., organizationally imposed, versus Intrinsic, e.g., desire to communicate through technology). Page et al. differentiate between functional motivations/barriers of use (which has been the focus of much research) versus social motivations/barriers to use. Other frameworks consider additional temporal states of adoption (whether they are currently using and whether they will in the future). See **[95]** for more detailed descriptions.

Guidelines for Designing Privacy-Sensitive Social Media

Now that you have learned about various privacy problems related to social media use, how do you apply that to designing or studying social media? Here are some practical guidelines.

Identifying Privacy Attitudes. Measuring privacy attitudes is a tricky task. Using existing informational privacy scales, users often say they are concerned, but this does not end up matching their actual behavior. By approaching it from a boundary regulation perspective, it will be easier to identify the proper balance between sharing too much and sharing too little. The survey items described in this chapter offer a way to measure concerns about boundary regulation as well as positive expectations. Considering both are key to more accurately predicting user behaviors.

Understanding Your Target Population. Some key characteristics are described in this chapter. Identifying these in your target population can help you be aware of individual differences that might affect privacy preferences on social media. When you are measuring privacy concerns, matching the preferences of your audience makes it more likely that they will have a good user experience. Pay particular attention to traits that have been identified as being related to usage and adoption of social media platforms, such as the FYI communication style which can be measured using the survey items provided in this chapter.

Evaluating Privacy Features. Focus on understanding whether users perceive your privacy features as useful or perhaps as posing a relational hindrance. The survey items provided in this chapter can help you do so. When anticipating privacy needs of your social media users, make sure you identify features that may impact boundary regulation both positively and negatively. You can compare attitudes between the existing feature and the newer version of the feature that will/has been deployed. You can also correlate attitudes towards privacy features with individual characteristics – some subpopulation of users may see privacy features as useful while others may consider them a relational hindrance.

Chapter Summary

Social media has been widely adopted and quickly become an integral part of social, personal, economic, political, professional, and instrumental welfare. Understanding how mediated social interactions change the assumptions around audience management, disclosure, and self-presentation are key to working towards reconciling offline privacy assumptions with new realities. Moreover, given the rapidly changing landscape of widely available social media platforms, researchers and designers need to continually re-evaluate the privacy implications of new services, features, and interaction modalities.

With the rise of networked individualism, an especially strong emphasis must be placed on understanding individual characteristics and traits that can shape a user's

privacy expectations and needs. Given the inherently social nature of social media, understanding social norms and the influence of larger cultural and structural factors is also important for interpreting expectations of privacy and the significance around various social media behaviors.

Privacy does not have a one-size-fits all solution. It is a normative construct that is context dependent and can change over time, from culture to culture, and person to person. It needs to be weighed across different individuals and against other important goals and values of the larger group or society. Because people and their social interactions can be complex, designing for social media privacy is usually not a straightforward task. However, the consequences of not addressing privacy issues can range from irritating to devastating. Using this chapter as a guide and taking the steps to think through privacy needs and expectations of your social media users, is an integral part of designing for social media.

References

1. A Acquisti and R Gross. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *Privacy Enhancing Technologies*: 36–58.

2. Ben Agger. 2015. *Oversharing: Presentations of Self in the Internet Age*. Routledge.

3. Ali Abdallah Alalwan, Nripendra P. Rana, Yogesh K. Dwivedi, and Raed Algharabat. 2017. Social media in marketing: A review and analysis of the existing literature. *Telematics and Informatics* 34, 7: 1177–1190.

4. Irwin Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Brooks/Cole Publishing Company, Monterey, CA.

5. Nazanin Andalibi. 2020. Disclosure, privacy, and stigma on social media: Examining non-disclosure of distressing experiences. *ACM Transactions on Computer-Human Interaction (TOCHI)* 27, 3: 1–43.

6. Nazanin Andalibi, Oliver L. Haimson, Munmun De Choudhury, and Andrea Forte. 2016. Understanding social media disclosures of sexual abuse through the lenses of support seeking and anonymity. *Proceedings of the 2016 CHI conference on human factors in computing systems*, 3906–3918.

7. Nazanin Andalibi, Pinar Ozturk, and Andrea Forte. 2017. Sensitive Self-disclosures, Responses, and Social Support on Instagram: the case of# depression. *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*, 1485–1500.

8. Andrew Torba. 2019. High School Teacher Fired For Tweets Criticizing Illegal Immigration. *Gab News*. Retrieved November 19, 2020 from https://news.gab.com/2019/09/16/high-school-teacher-fired-for-tweets-criticizing-illegal-immigration/.

9. Naveen Farag Awad and M. S. Krishnan. 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly* 30, 1: 13–28.

10. Oshrat Ayalon and Eran Toch. 2013. Retrospective privacy: managing longitudinal privacy in online social networks. *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, ACM Press, 1.

11. Mitja D. Back, Juliane M. Stopfer, Simine Vazire, et al. 2010. Facebook Profiles Reflect Actual Personality, Not Self-Idealization. *Psychological Science* 21, 3: 372–374.

12. Louise Barkhuus. 2012. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 367–376.

13. Lisa Barnard. 2014. The cost of creepiness: How online behavioral advertising affects consumer purchase intention. .

14. Frank R. Bentley and Crysta J. Metcalf. 2008. Location and activity sharing in everyday mobile communication. *Proceeding of the twenty-sixth annual CHI conference extended abstracts on Human factors in computing systems - CHI '08*, ACM Press, 2453.

15. Jens Binder, Andrew Howes, and Alistair Sutcliffe. 2009. The problem of conflicting social spheres: effects of network structure on experienced tension in social network sites. *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, ACM Press, 965.

16. Reuben Binns, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2018. Measuring Third-party Tracker Power Across Web and Mobile. *ACM Trans. Internet Technol.* 18, 4: 52:1-52:22.

17. Gwen Bouvier. 2015. What is a discourse approach to Twitter, Facebook, YouTube and other social media: connecting with other academic fields? *Journal of Multicultural Discourses* 10, 2: 149–162.

18. Danah Boyd. 2002. Faceted Id/Entity : managing representation in a digital world. Retrieved August 14, 2020 from https://dspace.mit.edu/handle/1721.1/39401.

19. Danah Boyd. 2006. *Friends, Friendsters, and MySpace Top 8: Writing Community Into Being on Social Network Sites*. First Monday.

20. Danah M. Boyd and Nicole B. Ellison. 2007. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* 13, 1: 210–230.

21. danah michele boyd. 2004. Friendster and publicly articulated social networking. *Extended abstracts of the 2004 conference on Human factors and computing systems - CHI '04*, ACM Press, 1279.

22. Michael J. Brzozowski, Tad Hogg, and Gabor Szabo. 2008. Friends and foes: ideological social networking. *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08*, ACM Press, 817.

23. Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science & Technology* 58, 2: 157–165.

24. Moira Burke, Cameron Marlow, and Thomas Lento. 2010. Social Network Activity and Social Well-being. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 1909–1912.

25. Caleb T. Carr and Rebecca A. Hayes. 2015. Social media: Defining, developing, and divining. *Atlantic journal of communication* 23, 1: 46–65.

26. Xi Chen and Shuo Shi. 2009. A literature review of privacy research on social network sites. *2009 International Conference on Multimedia Information Networking and Security*, IEEE, 93–97.

27. Hichang Cho, Bart Knijnenburg, Alfred Kobsa, and Yao Li. 2018. Collective Privacy Management in Social Media: A Cross-Cultural Validation. *ACM Trans. Comput.-Hum. Interact.* 25, 3: 17:1-17:33.

28. Tae Rang Choi and Yongjun Sung. 2018. Instagram versus Snapchat: Self-expression and privacy concern on social media. *Telematics and Informatics* 35, 8: 2289–2298.

29. Chris Clemens, David Atkin, and Archana Krishnan. 2015. The influence of biological and personality traits on gratifications obtained through online dating websites. *Computers in Human Behavior* 49: 120–129.

30. Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location Disclosure to Social Relations: Why, When, & What People Want to Share. 10.

31. Sauvik Das and Adam Kramer. 2013. Self-Censorship on Facebook. *Proceedings of the International AAAI Conference on Web and Social Media* 7, 1.

32. Jenny L Davis and Nathan Jurgenson. 2014. Context collapse: theorizing context collusions and collisions. *Information, Communication & Society* 17, 4: 476–485.

33. Isobel Asher Hamilton Dean Grace. Signal downloads skyrocketed 4,200% after WhatsApp announced it would force users to share personal data with Facebook. It's top of both Google and Apple's app stores. *Business Insider*. Retrieved February 1, 2021 from https://www.businessinsider.com/whatsapp-facebook-data-signal-download-telegram-encrypted-messaging-2021-1.

34. Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication* 15, 1: 83–108.

35. Vanessa P. Dennen, Stacey A. Rutledge, Lauren M. Bagdy, Jerrica T. Rowlett, Shannon Burnick, and Sarah Joyce. 2017. Context Collapse and Student Social Media Networks: Where Life and High School Collide. *Proceedings of the 8th International Conference on Social Media & Society - #SMSociety17*, ACM Press, 1–5.

36. Tobias Dienlin and Sabine Trepte. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology* 45, 3: 285–297.

37. Tamara Dinev, Massimo Bellotto, Paul Hart, Vincenzo Russo, Ilaria Serra, and Christian Colautti. 2006. Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems* 15, 4: 389–402.

38. Leyla Dogruel. 2019. Too much information!? Examining the impact of different levels of transparency on consumers' evaluations of targeted advertising. *Communication Research Reports* 36, 5: 383–392.

39. Claire Dolin, Ben Weinshel, Shawn Shan, et al. 2018. Unpacking perceptions of data-driven inferences underlying online targeting and personalization. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ACM, 493.

40. Erin Donnelly. 2019. Kim Kardashian mom-shamed over photo of North staring at a phone: "Give her a book." *Yahoo! Entertainment*. Retrieved April 11, 2021 from https://www.yahoo.com/entertainment/kim-kardashian-mom-shamed-north-west-phone-book-151126429.html.

41. Stefanie Duguay. 2016. “He has a way gayer Facebook than I do”: Investigating sexual identity disclosure and context collapse on a social networking site. *New Media & Society* 18, 6: 891–907.

42. Robin Dunbar. 2011. How many" friends" can you really have? *Ieee Spectrum* 48, 6: 81–83.

43. C. Dwyer, S.R. Hiltz, M.S. Poole, et al. 2010. Developing Reliable Measures of Privacy Management within Social Networking Sites. *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 1–10.

44. Kate Ehrlich and N. Shami. 2010. Microblogging Inside and Outside the Workplace. *Proceedings of the International AAAI Conference on Web and Social Media* 4, 1.

45. Nicole B. Ellison, Charles Steinfield, and Cliff Lampe. 2007. The Benefits of Facebook “Friends:” Social Capital and College Students’ Use of Online Social Network Sites. *Journal of Computer-Mediated Communication* 12, 4: 1143–1168.

46. Nicole B. Ellison, Charles Steinfield, and Cliff Lampe. 2011. Connection Strategies: Social Capital Implications of Facebook-enabled Communication Practices. *New Media & Society* 13, 6: 873–892.

47. Nicole B. Ellison, Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. 2011. Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment. In S. Trepte and L. Reinecke, eds., *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer, Berlin, Heidelberg, 19–32.

48. M. Fire, R. Goldschmidt, and Y. Elovici. 2014. Online Social Networks: Threats and Solutions. *IEEE Communications Surveys Tutorials* 16, 4: 2019–2036.

49. Simone Fischer-Hübner, Julio Angulo, Farzaneh Karegar, and Tobias Pulls. 2016. Transparency, Privacy and Trust–Technology for Tracking and Controlling My Data Disclosures: Does This Work? *IFIP International Conference on Trust Management*, Springer, 3–14.

50. Joshua Fogel and Elham Nehmad. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior* 25, 1: 153–160.

51. D Fono and K Raynes-Goldie. 2006. Hyperfriends and beyond: Friendship and social norms on Live Journal. *Internet research annual*.

52. Gerald Friedland and Robin Sommer. 2010. Cybercasing the Joint: On the Privacy Implications of Geo-Tagging. 6.

53. Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77: 226–261.

54. Martin Gibbs, James Meese, Michael Arnold, Bjorn Nansen, and Marcus Carter. 2015. #Funeral and Instagram: death, social media, and platform vernacular. *Information, Communication & Society* 18, 3: 255–268.

55. Jonathan Grudin. 2001. Desituating Action: Digital Representation of Context. *Human–Computer Interaction* 16, 2–4: 269–286.

56. Anatoliy Gruzd, Drew Paulin, and Caroline Haythornthwaite. 2016. Analyzing social media and learning through content and social network analysis: A faceted methodological approach. *Journal of Learning Analytics* 3, 3: 46–71.

57. Gaynor Hall and Courtney Gousman. 2020. Suburban teacher's social media post sparks outrage, internal investigation | WGN-TV. *WGNTV*. Retrieved November 19, 2020 from https://wgntv.com/news/chicago-news/suburban-teachers-social-media-post-sparks-outrage-internal-investigation/.

58. E Hargittai. 2007. Whose Space? Differences Among Users and Non-Users of Social Network Sites. *Journal of Computer-Mediated Communication* 13, 1.

59. Ki Mae Heussner and Dalia Fahmy. Teacher Loses Job After Commenting About Students, Parents on Facebook. *ABC News*. Retrieved November 19, 2020 from https://abcnews.go.com/Technology/facebook-firing-teacher-loses-job-commenting-students-parents/story?id=11437248.

60. Tad Hogg and D Wilkinson. 2008. Multiple Relationship Types in Online Communities and Social Networks. 6.

61. David J. Houghton and Adam N. Joinson. 2010. Privacy, Social Network Sites, and Social Relations. *Journal of Technology in Human Services* 28, 1–2: 74–94.

62. Mariea Grubbs Hoy and George Milne. 2010. Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising* 10, 2: 28–45.

63. Giovanni Iachello and Jason Hong. 2007. End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction* 1, 1: 1–137.

64. Adam N. Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B. Paine Schofield. 2010. Privacy, Trust, and Self-Disclosure Online. *Human–Computer Interaction* 25, 1: 1–24.

65. Yumi Jung and Emilee Rader. 2016. The Imagined Audience and Privacy Concern on Facebook: Differences Between Producers and Consumers. *Social Media + Society* 2, 2: 2056305116644615.

66. Gerald C. Kane, Maryam Alavi, Giuseppe (Joe) Labianca, and Stephen P. Borgatti. 2014. What'S Different About Social Media Networks? A Framework and Research Agenda. *MIS Quarterly* 38, 1: 275–304.

67. Pamela Karr-Wisniewski, David Wilson, and Heather Richter-Lipford. 2011. A new social order: Mechanisms for social network site boundary regulation. *Americas Conference on Information Systems, AMCIS*.

68. Asha Kaul and Vidhi Chaudhri. 2018. Do Celebrities Have It All? Context Collapse and the Networked Publics. *Journal of Human Values* 24, 1: 1–10.

69. B. P. Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies* 71, 12: 1144–1162.

70. Bart P. Knijnenburg, Elaine M. Raybourn, David Cherry, Daricia Wilkinson, Saadhika Sivakumar, and Henry Sloan. 2017. Death to the Privacy Calculus? *Proceedings of the 2017 Networked Privacy Workshop at CSCW*, Social Science Research Network.

71. Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64: 122–134.

72. Ksenia Koroleva, Hanna Krasnova, Natasha Veltri, and Oliver Günther. 2011. It's All About Networking! Empirical Investigation of Social Capital Formation on Social Network Sites. *ICIS 2011 Proceedings*.

73. Nicole C. Krämer and Nina Haferkamp. 2011. Online Self-Presentation: Balancing Privacy Concerns and Impression Construction on Social Networking Sites. In S. Trepte and L. Reinecke, eds., *Privacy Online:*

Perspectives on Privacy and Self-Disclosure in the Social Web. Springer Berlin Heidelberg, Berlin, Heidelberg, 127–141.

74. Nicole C. Krämer and Stephan Winter. 2008. Impression Management 2.0: The Relationship of Self-Esteem, Extraversion, Self-Efficacy, and Self-Presentation Within Social Networking Sites. *Journal of Media Psychology* 20, 3: 106–116.

75. Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: interpersonal management of disclosure in social network services. *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, ACM Press, 3217.

76. N. Li and G. Chen. 2010. Sharing location in online social networks. *IEEE Network* 24, 5: 20–25.

77. Yao Li, Bart P. Knijnenburg, Alfred Kobsa, and M-H. Carolyn Nguyen. 2015. Cross-Cultural Privacy Prediction. *Workshop "Privacy Personas and Segmentation", 11th Symposium On Usable Privacy and Security (SOUPS)*.

78. Han Lin, William Tov, and Lin Qiu. 2014. Emotional disclosure on social networking sites: The role of network structure and psychological needs. *Computers in Human Behavior* 41: 342–350.

79. Janne Lindqvist, Justin Cranshaw, Jason Wiese, Jason Hong, and John Zimmerman. 2011. I'm the mayor of my house: examining why people use foursquare - a social-driven location sharing application. *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, ACM Press, 2409.

80. Eden Litt. 2012. Knock, Knock. Who's There? The Imagined Audience. *Journal of Broadcasting & Electronic Media* 56, 3: 330–345.

81. Eden Litt and Eszter Hargittai. 2016. The Imagined Audience on Social Network Sites. *Social Media + Society* 2, 1: 2056305116633482.

82. Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4: 336–355.

83. Alice E. Marwick and danah boyd. 2011. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13, 1: 114–133.

84. Brendan Meeder, Jennifer Tam, Patrick Gage Kelley, and Lorrie Faith Cranor. 2010. RT @IWantPrivacy: Widespread Violation of Privacy Settings in the Twitter Social Network. 12.

85. Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79: 119–157.

86. Helen Nissenbaum. 2010. Privacy in Context. *Stanford University Press*.

87. Egle Oolo and Andra Siibak. 2013. Performing for one's imagined audience: Social steganography and other privacy strategies of Estonian teens on networked publics. *Institute of Journalism and Communication, University of Tartu, Tartu, Estonia* 7, 1.

88. Susanna Paasonen, Ben Light, and Kylie Jarrett. 2019. The dick pic: harassment, curation, and desire. *Social Media+ Society* 5, 2: 2056305119826126.

89. Ali Padyab and Tero Pã. Facebook Users Attitudes towards Secondary Use of Personal Information. 20.

90. Xinru Page, Reza Ghaiumy Anaraky, and Bart P. Knijnenburg. 2019. How communication style shapes relationship boundary regulation and social media adoption. *Proceedings of the 10th International Conference on Social Media and Society*, 126–135.

91. Xinru Page, Reza Ghaiumy Anaraky, Bart P. Knijnenburg, and Pamela J. Wisniewski. 2019. Pragmatic Tool vs. Relational Hindrance: Exploring Why Some Social Media Users Avoid Privacy Features. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW: 1–23.

92. Xinru Page, Bart P. Knijnenburg, and Alfred Kobsa. 2013. What a tangled web we weave: lying backfires in location-sharing social media. *Proceedings of the 2013 conference on Computer supported cooperative work - CSCW '13*, ACM Press, 273.

93. Xinru Page, Bart P. Knijnenburg, and Alfred Kobsa. 2013. FYI: communication style preferences underlie differences in location-sharing adoption and usage. *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, ACM, 153–162.

94. Xinru Page, Alfred Kobsa, and Bart P. Knijnenburg. 2012. Don't Disturb My Circles! Boundary Preservation Is at the Center of Location-Sharing Concerns.

Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media, 266–273.

95. Xinru Page, Pamela Wisniewski, Bart P. Knijnenburg, and Moses Namara. 2018. Social Media's Have-Nots: An Era of Social Disenfranchisement. *Internet Research* 28, 5.

96. Xinru Woo Page. 2014. *Factors That Influence Adoption and Use of Location-Sharing Social Media*. University of California, Irvine.

97. Leysia Palen and Paul Dourish. 2003. Unpacking "Privacy" for a Networked World. *NEW HORIZONS* 5: 8.

98. Paul A Pavlou. 2011. State of the Information Privacy Literature: Where Are We Now and Where Should We Go. *MIS Quarterly* 35, 4: 977–988.

99. Sandra Petronio. 1991. Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. *Communication Theory* 1, 4: 311–335.

100. Pew Research Center. 2019. Social Media Fact Sheet. *Pew Research Center: Internet, Science & Tech*. Retrieved November 27, 2020 from https://www.pewresearch.org/internet/fact-sheet/social-media/.

101. Jacqueline C. Pike, Patrick J. Bateman, and Brian S. Butler. 2018. Information from social networking sites: Context collapse and ambiguity in the hiring process. *Information Systems Journal* 28, 4: 729–758.

102. Kathrynn Pounders, Christine M. Kowalczyk, and Kirsten Stowers. 2016. Insight into the motivation of selfie postings: impression management and self-esteem. *European Journal of Marketing* 50, 9/10: 1879–1892.

103. Anabel Quan-Haase and Alyson L. Young. 2010. Uses and gratifications of social media: A comparison of Facebook and instant messaging. *Bulletin of science, technology & society* 30, 5: 350–361.

104. Lee Rainie and Barry Wellman. 2012. *Networked*. MIT Press, Cambridge, MA.

105. Kopo M. Ramokapane, Gaurav Misra, Jose M. Such, and Sören Preibusch. 2021. Truth or Dare: Understanding and Predicting How Users Lie and Provide Untruthful Data Online. .

106. Karl van der Schyff, Stephen Flowerday, and Steven Furnell. 2020. Duplicitous social media and data surveillance: An evaluation of privacy risk. *Computers & Security* 94: 101822.

107. Reinhard Selten. 1990. Bounded rationality. *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft* 146, 4: 649–658.

108. Kim Bartel Sheehan. 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 13, 4: 24–38.

109. Christopher Sibona. 2014. Unfriending on Facebook: Context Collapse and Unfriending Behaviors. *2014 47th Hawaii International Conference on System Sciences*, 1676–1685.

110. Manya Sleeper, Rebecca Balebako, Sauvik Das, Amber Lynn McConahy, Jason Wiese, and Lorrie Faith Cranor. 2013. The post that wasn't: exploring self-censorship on facebook. *Proceedings of the 2013 conference on Computer supported cooperative work*, ACM, 793–802.

111. Hilary Smith, Yvonne Rogers, and Mark Brady. 2003. Managing one's social network: Does age make a difference. *In: Proc. Interact 2003, IOS*, Press, 551–558.

112. Daniel Solove. 2008. *Understanding Privacy*. Harvard University Press, Cambridge, MA.

113. Anthony Stefanidis, Andrew Crooks, and Jacek Radzikowski. 2011. Harvesting ambient geospatial information from social media feeds. .

114. Fred Stutzman and Woodrow Hartzog. 2012. Boundary Regulation in Social Media. 10.

115. Fred Stutzman and Jacob Kramer-Duffield. 2010. Friends only: examining a privacy-enhancing behavior in facebook. *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, ACM Press, 1553.

116. Jeannette Sutton, Leysia Palen, and Irina Shklovski. 2008. Backchannels on the Front Lines: Emergent Uses of Social Media in the 2007 Southern California Wildfires. 9.

117. Iraklis Symeonidis, Gergely Biczók, Fatemeh Shirazi, Cristina Pérez-Solà, Jessica Schroers, and Bart Preneel. 2018. Collateral damage of Facebook third-party applications: a comprehensive study. *Computers & Security* 77: 179–208.

118. Karen P. Tang, Jialiu Lin, Jason I. Hong, Daniel P. Siewiorek, and Norman Sadeh. 2010. Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. *Proceedings of the 12th ACM international conference on Ubiquitous computing*, ACM, 85–94.

119. The University of Central Florida, Pamela Wisniewski, A. K. M. Najmul Islam, et al. 2016. Framing and Measuring Multi-Dimensional Interpersonal Privacy Preferences of Social Networking Site Users. *Communications of the Association for Information Systems* 38: 235–258.

120. Janice Y Tsai, Patrick Gage Kelley, Lorrie FAith Cranor, and Norman Sadeh. Location-Sharing Technologies: Privacy Risks and Controls. 34.

121. Zeynep Tufekci. 2008. Grooming, Gossip, Facebook and Myspace. *Information, Communication & Society* 11, 4: 544–564.

122. Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, useful, scary, creepy: perceptions of online behavioral advertising. *proceedings of the eighth symposium on usable privacy and security*, ACM, 4.

123. José Van Dijck. 2012. Facebook as a tool for producing sociality and connectivity. *Television & New Media* 13, 2: 160–176.

124. Jessica Vitak. 2015. Balancing Audience and Privacy Tensions on Social Network Sites. 20.

125. Jessica Vitak and Nicole B. Ellison. 2013. 'There'sa network out there you might as well tap': Exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. *New media & society* 15, 2: 243–259.

126. Jessica Vitak, Cliff Lampe, Rebecca Gray, and Nicole B Ellison. "Why won't you be my Facebook friend?": strategies for managing context collapse in the workplace. 3.

127. Alan Westin. 1991. *Harris-Equifax Consumer Privacy Survey*. Equifax Inc, Atlanta, GA.

128. Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I Hong, and John Zimmerman. 2011. Are you close with me? are you nearby?: investigating social groups, closeness, and willingness to share. *UbiComp*: 10.

129. Daricia Wilkinson, Paritosh Bahirat, Moses Namara, et al. 2019. Privacy at a Glance: Exploring the Effectiveness of Screensavers to Improve Privacy Awareness. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI). Under Review*, ACM.

130. Daricia Wilkinson, Moses Namara, Karishma Patil, Lijie Guo, Apoorva Manda, and Bart Knijnenburg. 2021. *The Pursuit of Transparency and Control: A Classification of Ad Explanations in Social Media*. .

131. Pamela Wisniewski, A.K.M. Najmul Islam, Bart P. Knijnenburg, and Sameer Patil. 2015. Give Social Network Users the Privacy They Want. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, 1427–1441.

132. Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: coping mechanisms for sns boundary regulation. *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*, ACM Press, 609.

133. Sally ME Wyatt. 2003. Non-users also matter: The construction of users and non-users of the Internet. *Now users matter: The co-construction of users and technology*: 67–79.

134. Feng Xu, Katina Michael, and Xi Chen. 2013. Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research* 13, 2: 151–168.

135. Heng Xu, Tamara Dinev, H. Smith, and Paul Hart. 2008. *Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View*. .

136. Heng Xu and Sumeet Gupta. 2009. The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets* 19, 2–3: 137–149.

137. Heng Xu, Rachida Parks, Chao-Hsien Chu, and Xiaolong (Luke) Zhang. 2010. Information Disclosure and Online Social Networks: From the Case of Facebook News Feed Controversy to a Theoretical Understanding. *AMCIS*, Citeseer, 503.

138. Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2012. Research note-effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research* 23, 4: 1342–1363.

139. Huining Yang. 2020. Secondary-school Students' Perspectives of Utilizing Tik Tok for English learning in and beyond the EFL classroom. *2020 3rd International Conference on Education Technology and Social Science (ETSS 2020)*, 163–183.

140. Dmitry Zinoviev and Vy Duong. 2009. Toward Understanding Friendship in Online Social Networks. *arXiv:0902.4658 [cs]*.

141. 2018. Facebook and Instagram introduce time limit tool. *BBC News*. Retrieved February 10, 2021 from https://www.bbc.com/news/newsbeat-45030712.

142. Social Media Users. *DataReportal – Global Digital Insights*. Retrieved March 16, 2021 from https://datareportal.com/social-media-users.

143. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites - Zeynep Tufekci, 2008. Retrieved January 29, 2021 from https://journals.sagepub.com/doi/abs/10.1177/0270467607311484?casa_token=eRyqfkWa_psAAAAA%3A44Jmi3Z6bR8BMYvdaALVkLpcNqnA5oaTlteICGTXRImdmAVtVRnnI6qU2PwVK5Ahc2MNA8V4vFdpXA&.

144. Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? - Petronio - 2010 - Journal of Family Theory & Review - Wiley Online Library. Retrieved January 29, 2021 from https://onlinelibrary.wiley.com/doi/full/10.1111/j.1756-2589.2010.00052.x?casa_token=MzmOZZ0zepMAAAAA%3Al4I9p-z7T-h5TY7EHPbUuoF43bF-pRWm_Fua8-0WmnwRXDXewkrYjtpoeB-J23QYAeB7oXTv2VUti9dt.