Modeling User Characteristics Associated with Interdependent Privacy Perceptions on Social Media

MARY JEAN AMON

University of Central Florida

AARON NECAISE

University of Central Florida

NIKA KARTVELISHVILI

University of Central Florida

ANEKA WILLIAMS

University of Central Florida

YAN SOLIHIN

University of Central Florida

APU KAPADIA

Indiana University

‘Interdependent’ privacy violations occur when users share private photos and information about other people in social media without permission. This research investigated user characteristics associated with interdependent privacy perceptions, by asking social media users to rate photo-based memes depicting strangers on the degree to which they were too private to share. Users also completed questionnaires measuring social media usage and personality. Separate groups rated the memes on shareability, valence, and entertainment value. Users were less likely to share memes that were rated as private, except when the meme was entertaining or when users exhibited dark triad characteristics. Users with dark triad characteristics demonstrated a heightened awareness of interdependent privacy and increased sharing of others’ photos. A model is introduced that highlights user types and characteristics that correspond to different privacy preferences: privacy preservers, ignorers, and violators. We discuss how interventions to support interdependent privacy must effectively influence diverse users.

CCS CONCEPTS • Security and privacy ~ Human and societal aspects of security and privacy ~ Social aspects of security and privacy • Human-centered computing ~ Human computer interaction (HCI) ~ HCI design and evaluation methods~User studies • Social and professional topics ~ User characteristics

Additional Keywords and Phrases: Cluster analysis, dark triad, interdependent privacy, memes, sharing decisions, social media

1 INTRODUCTION

‘Interdependent privacy’ violations occur when social media users share private photos or information about other people without permission. These violations of other people’s privacy occur on a massive scale, as users post others’ embarrassing moments, identifying information, photos taken without permission, medical and sexual histories, and other sensitive content. Although research has found that

1073-0516/2023/1-ART1 $15.00
http://dx.doi.org/10.1145/3577014

people typically want to provide consent before people post information about them [79], users often do not ask for such permission before posting about other people [87].

Interdependent privacy violations are a primary threat associated with social media with wide-ranging consequences for victims. Information shared online is both persistent and cumulative, creating a repository of information that can be used by other people, sometimes for nefarious purposes [6,111]. Victims of interdependent privacy violations experience increased vulnerability and decreased autonomy, which is often accompanied by psychological distress and other personal and professional consequences ranging from extortion, harassment, identity theft, and stalking [78,83]. Although users can report inappropriate content, information spreads quickly within social media and across platforms, and social media corporations' practices for managing flagged material is limited [90,93].

The sources of interdependent privacy violations are numerous. For example, internet "trolls" direct their efforts toward upsetting or provoking others, often for no other reason than their own entertainment [73]. However, even well-intentioned users participate in privacy-violating behaviors due to lapses in judgment, insufficient information, inconsistent or underdeveloped standards of privacy, and emotionally driven decision-making [113]. Nonetheless, some users act in ways intended to preserve the privacy of others. Users may respond to existing privacy violations by flagging the inappropriate content for possible removal, "calling out" people who post inappropriate content, or purposefully ignoring information to save others from further embarrassment [88].

Interdependent privacy violations are part of the social media status quo and users vary in their propensity for protecting, ignoring, or violating the privacy of others. Despite the scope of interdependent privacy violations, a significant portion of the privacy literature focuses on measures to protect one's own privacy, and less is known about characteristics that drive users to protect versus violate others' privacy online. Prior literature examining user characteristics associated with interdependent privacy decisions has been limited to examining a small number of dimensions, for example, humor [40], gender, or personal privacy preferences [3]. Moreover, although prior work gestures at the notion that users display distinct privacy preferences, research in this area typically examines normative or "average" user attitudes and behaviors [46]. A more holistic account of interdependent privacy perceptions and user characteristics is critical, as interdependent privacy interventions rest on the ability to effectively identify and influence diverse users. Thus, interdependent privacy research must account for different types of users that vary in their interdependent privacy preferences, as well as their motivation for sharing and re-sharing on social media.

Accordingly, this research examines the extent to which user personality characteristics, social media behaviors, and demographic factors predict interdependent privacy perceptions, or the degree to which social media content depicting strangers' potentially private information is considered "too private" to share. We asked 245 regular social media users living in the United States to rate 68 real-world photo-based memes—which included potentially compromising photos of strangers—on the degree to which each meme was "too private to share on social media." Photo-based memes were systematically categorized and selected for the study using a modified thematic approach (§ 3.1.2 for details). Participants were then surveyed on several personality dimensions, self-reported social media usage, and demographic background. Separate participant groups rated the photo-based memes on shareability, valence, and entertainment value to identify how the memes' features interact with user characteristics to predict privacy perceptions. In addition to providing a descriptive overview of users' interdependent privacy perceptions on social media, we examine results from a series of statistical models aimed at better understanding user characteristics that predict interdependent privacy perceptions. Lastly, we identify distinct user types who differ based on interdependent privacy preferences, personality dimensions, and social media usage.

Our research complements previous interdependent privacy literature by examining content—specifically about other people—that users consider too private to share on social media, representing an important first step in aligning content moderation strategies (i.e., methods for monitoring and managing user-generated content) with users' privacy preferences. To be effective, content moderation strategies must accurately reflect the attitudes and behaviors of social media users toward interdependent privacy violations. Alignment between content moderation practices and public privacy perceptions is necessary for both avoiding false positives (e.g., punishment of socially acceptable social media behaviors) and false negatives (e.g., failure to prevent or minimize harmful behavior). Building on prior work that often focuses on normative interdependent privacy perceptions [46], we identify distinct user types that vary in their interdependent privacy perceptions and key psychosocial features that differentiate between them. For example, it is possible that research focusing on normative behavior neglects the needs of those most interested in privacy preservation because different types of users hold distinct interdependent privacy preferences.

Our research focuses on privacy perceptions regarding real-world photo-based memes that depict people. While online privacy violations can take many forms, photo-based memes are especially aligned with the topic of interdependent privacy, as they often include an identifiable image of a stranger, where it is unclear whether the stranger has consented to having their image altered, replicated, and spread publicly, and photos tend to be especially evocative and incriminating [8,55]. The text captions that often accompany memes provide a shared understanding that enables users to interpret the meme similarly, and the captions support general interest in the stimuli as attention-grabbing and potentially re-shareable on social media (i.e., versus a stand-alone image of a stranger). Thus, memes represent a popular real-world phenomenon that often operate as a vehicle for spreading *potentially* sensitive content about other people, and they are an appropriate point of reference point for a general audience examining potential interdependent privacy perceptions.

2 BACKGROUND

2.1 Interdependent Privacy Violations

Interdependent privacy is an umbrella term used to refer to a broad class of privacy risks that an individual incurs by virtue of other people's sharing decisions and can include the sharing of genetic data, statistical inference of otherwise undisclosed user characteristics based on social connections, and social media corporations having access to individual information due to social connections [46]. A relatively common form of interdependent privacy violations occurs when social media users share multimedia content including audio recordings, photos, and videos of other people on social media without permission (i.e., multimedia interdependent privacy [46]). A survey by Henne and colleagues [42] revealed that 52% of social media users learned by chance about photos of themselves online, including instances where photos were shared by strangers. Threats to interdependent privacy also come from close connections, with research by Besmer and Lipford [8] indicating that users' primary interdependent privacy concerns are regarding family and friends' sharing information out-of-context, especially if the information portrays the user in an unflattering light or shows them violating social norms.

Multi-party privacy (MPP) concerns are one class of interdependent privacy risks posed by the sharing of co-owned images by acquaintances or family members [46,60,104]. Dealing with MPP concerns can be difficult because the decision to share co-owned or group photos is made by a single individual, even though those depicted can have conflicting privacy preferences or may not participate in social media themselves [104]. Ideally, users would adopt collaborative strategies for addressing MPP concerns by discussing their preferences, seeking consent, or removing images contributing to the concerns [8,120]. However, this type of collaborative behavior is not the norm, and social media platforms provide limited tools for addressing MPP issues [46]. Given that family and friends have greater access to an individual's personal information, MPP concerns generated by close connections may be perceived as a greater threat to 'contextual integrity', as these individuals can move private information to the public sphere where the information may be shared with unintended audiences or the subject's portrayal may be altered [80].

Interdependent privacy risks extend beyond MPP concerns, as users also share pictures and videos of strangers for entertainment despite not owning that content themselves. A portion of interdependent privacy violations take the form of viral memes, or units of information that are transmitted widely and replicated over time, within social networks [98]. Photo-based memes often include personally identifying information, such as a photo subject's face, as well as information or comments about the featured individual. Notably, definitions of what constitutes 'private' information in the context of IDP violations vary and can include information about a person's demographic background or relationships [30,100,107] or even their drug activity, medical history, sexual history, embarrassing moments, or shaming people for non-normative behaviors [113]. In the case of social media users re-sharing photo-based memes that depict strangers, it is often impossible for the sharer to know if the person depicted consented to having their photo used as a meme, let alone aspects of the subject's privacy preferences. Thus, the resharing of photo-based memes that depict strangers can be seen as a potential IDP violation, where the impact of sharing is not immediately ascertainable.

Privacy violations are rated as more severe based on the degree to which victims lack control over their information [14], suggesting that the 'memeification' of an individual's personal information is a particularly significant threat to privacy on social media. Users may change the original photo or information as it spreads, or the meme may be transformed into an image macro as text captions are added to a photo [122]. Memes can be created or altered to portray people differently, with some memes highlighting people's positive traits and accomplishments and other memes showing people's negative traits or behaviors that violate social norms. In this way, memes serve as a vehicle through which private information about people is spread to unintended audiences and taken out of context [10,11,80] as a low-tech form of misinformation that influences public opinion [26]. As memes are shared at a micro-level, their spread contributes to macro-level social perceptions, influencing mindsets and behaviors of social groups [63,98]. Thus, the sharing and re-sharing of memes online can mean that the person depicted in the meme may have little to no control over how information about them is transmitted or how they are portrayed within large social networks.

Introduced before the advent of the internet, Westin's [114] classic theory of the four states of privacy remains relevant to modern-day privacy issues, especially so in the case of interdependent privacy. Put in today's context, Westin's dimension of 'solitude' or being free from others' observation is relevant to individuals' right to feel unencumbered by the threat of cameras and recording devices. Individuals also have the right to 'reserve,' or protection from unwanted intrusion upheld by the willing discretion of those surrounding the individual. Additional facets of Westin's model of privacy pertain to protection by close connections (i.e., 'intimacy') and strangers (i.e., 'anonymity' when in public spaces), highlighting that privacy is part of a communitarian process [62,75]. However, this shared responsibility for protecting one another's privacy is made more difficult when users vary in their privacy-relevant perceptions and decisions on social media.

2.2 Personality and Privacy Management

Research in self-disclosure on social media indicates that users and content interact to determine photo sharing decisions, where research often examines the effect of either user dispositions or situational factors in driving personal sharing decisions [55]. For example, people who rate themselves as open (versus private), post photos of other people more frequently, and those who openly admit to posting embarrassing photos of family and friends are more likely to share photo-based memes [3]. In terms of user personality profiles, research utilizing the Big Five model of personality dimensions has linked low agreeableness, high extraversion, and high neuroticism to deliberate cyberbullying, which often entails commenting to or about others without permission [5,17,28,31].

The Dark Triad (DT) model of personality [61,84] has also been used to understand social media misbehaviors [5,19,29,34]. The DT model focuses on the malevolent personality traits of Machiavellianism, narcissism, and psychopathy. Machiavellianism refers to a manipulative personality style, where people act in calculating, deceitful, and self-serving ways to gain power and enhance personal outcomes. People high in subclinical narcissism tend to be self-focused and motivated to improve and enhance their self-esteem with a high degree of dominance, entitlement, and grandiosity. Subclinical psychopathy refers to impulsivity and thrill-seeking combined with low levels of empathy and anxiety. Taken together, individuals high in DT traits are exploitative, apathetic, and willing to harm others for their own benefit [51,84].

DT traits are associated with the use of social media as a means for gossiping, increasing social capital, and monitoring social connections [116]. Machiavellians and narcissists tend to use social media to improve their image, with Machiavellians being especially calculated and disciplined in their posting behaviors [12,76,92]. This contrasts the impulsive behavior of more psychopathic users, who are more likely to act out their negative behaviors to harm others. Psychopathy is more strongly associated with trolling behavior than Machiavellianism or narcissism [5,68], such that people high in psychopathy are more likely to repeatedly communicate hostile and aggressive messages with the intention of causing distress. In this way, psychopathy is associated with intrusions upon others within their social networks, including with higher rates of unsolicited internet pornography [99]. Thus, Machiavellianism and narcissism tend to be associated with self-enhancing online behaviors, whereas psychopathy is related to other-harming online behaviors.

A significantly smaller body of literature examines online activity in terms of the Light Triad (LT) personality dimensions, or personality traits reflecting a beneficent orientation toward others, including faith in humanity (believing in the goodness of others), humanism (valuing the dignity and worth of others), and Kantianism (treating others as ends unto themselves) [57]. Kaufman and colleagues [57] respond to the rather extensive literature on the DT model by noting the importance of research that includes measures of both adaptive and maladaptive traits in the same study to represent the “full capacities of humanity.” Research examining LT personality dimensions in the context of online social connections shows that individuals high in LT traits are less likely to use dating or “hookup” apps like Tinder (esp. those high in Kantianism) and, when they do, are more likely to seek out long-term relationships [97]. Additionally, a recent study by March & Marrington [72] reports that all three dimensions of the LT are associated with self-reported “prosocial" online behaviors (e.g., using the internet to feel closer to others), while Kantianism is associated with decreased “antisocial” online behaviors (e.g., using the internet to show off).

Notably, prior research does not elucidate the extent to which individuals high in DT and LT recognize other social media users’ right to privacy. Given that DT traits are defined, in part, by an apathy toward others [51,112], it is possible that high-DT users are relatively insensitive to the potentially private nature of online content and, therefore, rate such content as less private than other users. On the other hand, high-DT individuals are also defined by manipulativeness (i.e., Machiavellianism) and intent to harm (i.e., psychopathy), suggesting that high-DT users may be acutely aware of information that can be used against other people. Given the comparatively small body of literature on LT dimensions, more research is needed to understand how LT dimensions correspond to social media attitudes and behaviors in general, including interdependent privacy perceptions and related behaviors.

We anticipate that DT and LT will support a new understanding of distinct types of interdependent privacy perceptions among social media users. Revisiting Westin’s [114] model of privacy (§ 2.1), Westin expressed an uncertainty of individuals’ desire for privacy, which he referred to as a privacy paradox. He managed the conflict between individuals’ need for privacy and privacy-violating behaviors by categorizing individuals as privacy pragmatists, fundamentalists, or unconcerned. Whereas the privacy unconcerned group tends to focus on the benefits of information sharing, and the privacy fundamentalists focus on the drawbacks of information sharing, pragmatists rationally negotiate their privacy within the context of a marketplace [75,115]. Westin’s model has been criticized for identifying consumers as rational in their decision-making, with opposing work highlighting consumers as generally unaware of privacy practices and rules in the marketplace with overly-optimistic and flawed rationale for privacy decisions [109]. Despite its limitations, Westin’s model remains influential in the privacy literature and suggests that social media users are likely to demonstrate diverse interdependent privacy preferences—to date, this connection remains untested.

2.3 Study Overview

The current paper focuses on identifying user characteristics that are associated with different interdependent privacy perceptions and behaviors on social media. In Study 1, we assessed 245 regular social media users from the United States on the degree to which they considered real-world photo-based memes as too private to share on social media, with the memes depicting strangers in more-or-less privacy-compromising circumstances. We used a modified thematic approach to categorize and select memes to ensure that the memes depicted a range of potentially sensitive issues. Memes ranged from showing people who were apparently unaware their photo was being taken, illicit drug activity, shaming images of people behaving against social norms, and sensitive documents that were posted on social media (e.g., licenses and passports). Additional memes included images of strangers that do not appear to be derogatory, embarrassing, or sensitive, though it remains an open question as to the extent to which users find it acceptable to share any photos of strangers without permission. Participants also completed questionnaires assessing personality traits, social media usage behaviors, and demographic characteristics. Finally, in a follow-up study (referred to as "Study 2" below), additional independent groups of participants rated the perceived entertainment value, shareability, and valence (i.e., how positively or negatively the photo target was portrayed) of the same set of memes presented in Study 1. These participant ratings were averaged such that each meme in the dataset had a single value for perceived entertainment, shareability, and valence. This allowed us to assess how subjective meme features (e.g., their entertainment value) interacted with user characteristics to predict the degree to which a meme was perceived as private. In addition to characterizing "normative" or average interdependent privacy perceptions, we utilized cluster analysis to identify distinct user types that vary in their perceptions. Thus, we examine key features of social media posts that modulate privacy perceptions, user characteristics associated with interdependent privacy perceptions, and variability in users' interdependent privacy perceptions.

H1: Because prior research suggests that shareability and privacy saliency can be anticorrelated [3], we hypothesized that privacy perceptions and sharing likelihood ratings of photo-based memes would not be strongly related. Furthermore, we expected that an anticorrelation between sharing likelihood and privacy would be lessened when accounting for meme entertainment value and valence.

H2: We hypothesized that high-DT users would report sharing more photos of themselves and other people online, a finding that would be in line with prior work indicating increased self-disclosure and intrusive acts toward others by DT personality types [74,95,96].

H3: Given that DT characteristics are associated with a willingness to exploit and harm others for one's own benefit [51,84], we hypothesized that high-DT users would rate photo-based memes as less private than other users.

H4: Lastly, consistent with Westin's [115] model of privacy, we hypothesized that three user types would vary in their interdependent privacy perceptions and behaviors. However, the validity of Westin's 'privacy pragmatist' group has been questioned, and we expected there would be a group of high-DT privacy violators instead.

3 METHOD

3.1 Stimuli

The photo-based memes were identified from a large number of memes that depicted people, which were visually scanned and downloaded by multiple researchers from popular social media sites, including Twitter, Reddit, and Pinterest by searching generally for ‘memes’ in each site. This initial set of memes was narrowed to include only photos that clearly portrayed at least one person and contained a text caption of 50 words or less to provide context understandable to a general audience. The combination of image and text caption reflects photo-based memes commonly circulated on social media, which often contain photos and information about strangers. Given that this study does not focus on prejudice, we excluded memes that involved sexist, racist, or otherwise bigoted themes. We also excluded well-known celebrities to ensure our participants focused on privacy violations of ordinary individuals. In addition, we attempted to include individuals from apparently diverse ages, genders, and racial and ethnic backgrounds in our sample of memes.

The memes differed in the type of potential privacy violation they represented, such that each meme represented one of 13 categories (see Table 1). For example, a meme depicting an inebriated person with a liquor bottle in their hand was included in the “drug use” category, as this aspect of the meme appeared particularly salient and sensitive to the independent coders. Another meme showed a person’s license with an entertaining caption, which was included in the “personal information” category, due to a license being considered a sensitive personal document. Meme categories were generated using a modified thematic approach, which provides a framework for qualitative analysis of themes within data. After gathering hundreds of photo-based memes that fit the criteria (e.g., portrayal of a person with text caption; no celebrities), two coders engaged in a constant comparative method whereby memes were assigned to categories based on content and then compared with other memes included in the same category. New categories were generated if identified memes needed to be further differentiated or if categories could be combined. This method allowed us to uncover a range of categories representing potentially sensitive information about others contained within photo-based memes. The iterative process and final categories were picked when saturation was reached, and no new themes emerged. The two independent coders compared their coding and agreed to the final framework via consensual validation [2]. We also referred to resources such as articles from Li and colleagues [66] and to Mao and colleagues [71] throughout the process to ensure that our conceptualization of potentially sensitive information aligned with prior work.

Finally, we narrowed down the number of memes in each category to between three and six exemplar stimuli, with a total of 68 memes. The final number of memes per category was selected for two key reasons: 1) Anticipating that groups of participants would be rating each meme in addition to completing questionnaires, we kept in mind the potential for rating fatigue should too many memes be included. 2) Although some categories (e.g., insulting) had many memes, other categories (e.g., personal information) had fewer memes or the memes were highly similar to one another. We opted to have a similar number of memes per group, thus reducing the size of the stimuli set. The final memes retained for each category were selected based on the degree to which they clearly aligned with the category theme and depicted diverse photo subjects. Table 1 provides detailed information about the categories. For example, some photo subjects appear unaware they were being photographed, let alone made into a meme for social media; we refer to these memes as “Candid.” One such meme from this category portrayed a man sitting in a subway train with his chest and stomach exposed with the caption, “My main goal in life is to be as comfortable as this man is on the subway.” The control category consisted of images that do not appear to violate the subject’s privacy. Thus, while all memes contained information about strangers, it was assumed that they would vary in the degree to which they would be considered private.

Table 1: Types of photo-based memes depicted during the meme rating tasks. Average and standard deviation of privacy ratings from participants in Study 1 are included for each category, where higher ratings indicated the meme was perceived as more private.

Category Name	Number of Memes	Category Description	Privacy Rating *M* (*SD*)
Candid	6	Individual appears to be unaware their photo was taken	2.68 (0.24)
Children	6	Child portrayed in negative or positive light	2.72 (0.28)
Out-of-Context	5	Photo taken out of context through addition of text caption	2.45 (0.16)
Drug Use	5	Photo or text highlights individual’s drug or alcohol use	3.05 (0.57)
Insulting	5	Photo accompanied by derogatory message	2.87 (0.25)
Location Information	5	Photo or text caption reveals details of subject’s location	2.56 (0.14)
Medical Information	5	Photo or text caption reveals personal medical information	2.70 (0.19)
Online Activity	5	Aspects of online activity, such as dating profile or search history	3.07 (0.55)
Personal Information	5	Identifying personal information, such as driver’s license or passport	4.00 (0.22)
Sexual History	5	Details of sexual history	3.45 (0.18)
Shaming	5	‘Calling out’ someone’s socially unacceptable behavior	2.84 (0.20)
Work/School Misbehavior	6	Potentially reprimandable behaviors at work or school	2.89 (0.55)
Control	5	Control category portraying people in a positive or neutral light	2.50 (0.13)

3.2 Questionnaires

In Study 1 (coding for perceived privacy of memes) and Study 2 (coding for perceived entertainment, shareability, and valence), participants completed a series of questionnaires collecting data about their demographic background, social media usage, and personality traits. These questionnaires are described in detail below.

Social Media Usage Questionnaire. The Social Media Usage Questionnaire consists of seven questions targeting participants’ online photo sharing behaviors. Participants used an eight-point Likert scale to rate the frequency with which they share or re-share photos on social media, including the frequency with which they share or re-share pictures taken by them, their friends, or their family versus the frequency with which they share or re-share pictures that they find on the internet (1=Never; 8=Multiple times in a day). In addition, participants indicated their typical target audience (i.e., friends/connections, general viewers/public, or both), the social media platforms to which they share most often (see § 3.1), and if they share their own photos more or re-share other people’s photos more often (including the option “I share and re-share equally”).

Social Media Disorder Scale (SMD). This version of the Social Media Disorder Scale consists of nine items pertaining to disordered social media use [23]. Participants used Likert scales to indicate the frequency with which they experience potentially problematic attitudes and behaviors pertaining to social media (1 = never, 5 = always), such as trying to spend less time on social media but failing or frequently using social media to escape from negative feelings. It should be noted that the original nine-item SMD scale [23] asked participants to respond to each statement with a "yes" or "no." The scale was altered for the current study to have Likert-like responses to maintain consistency with other measures in the study.

A Brief Version of the Big Five Personality Inventory (BFI-10). This version of the Big Five Personality Inventory is a ten-item scale that describes participants' personality across dimensions of extraversion, agreeableness, conscientiousness, neuroticism, and openness. The BFI-10 demonstrated acceptable levels of reliability and validity compared to the full 44-item scale [86]. Each subscale includes one standard-scored and one reverse-scored item, such as "I see myself as someone who is outgoing, sociable" (extraversion, standard-scored) and "I see myself as someone who is reserved" (extraversion, reverse-scored). Participants were asked to rate their extent of agreement with each statement using a five-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree).

Short Dark Triad Scale (SD3). The Short Dark Triad Scale was used to measure participants' expression of three closely related dimensions of personality referred to as the "dark triad" (due to their malevolent nature). The brief version has shown satisfactory levels of reliability and validity compared to longer measures [53]. Participants were asked to rate via Likert scales their extent of agreement with 27 statements associated with the Machiavellianism, narcissism, and psychopathy personality traits (1 = Strongly Disagree; 5 = Strongly Agree). The Machiavellianism subscale includes statements pertaining to manipulative behaviors, such as "I like to use clever manipulation to get my way" and "You should wait for the right time to get back at people." The narcissism subscale includes statements such as "I hate being the center of attention" (reverse-scored) and "I know that I am special because everyone keeps telling me so." Finally, the psychopathy subscale includes statements related to anti-social and emotionally callous behaviors such as "I like to get revenge on authorities" and "payback needs to be quick and nasty."

Light Triad Scale (LTS). This questionnaire consists of twelve items and measures participants' LT personality traits (i.e., faith in humanity, humanism, and Kantianism) [57]. The traits measured by the LTS are in many ways opposite to those measured by the SD3 and reflect the benevolent, authentic, and hopeful aspects of human nature. The faith in humanity subscale includes items such as "I tend to see the best in people" and "I think people are mostly good." The humanism subscale includes items such as "I tend to admire others" and "I tend to treat others as valuable." Finally, the Kantianism subscale consists of items such as "I prefer honesty over charm" and "I don't feel comfortable overtly manipulating people to do something I want." Participants were asked to rate their extent of agreement with each statement in the questionnaire (1 = Strongly Disagree; 5 = Strongly Agree).

Privacy Preference Question. This measure consisted of a single question: "Are you a private person who keeps to yourself, or an open person who enjoys sharing with others? [43]" Participants were asked to answer using a seven-point Likert scale (1=Very Private; 7=Very Open).

3.3 Study 1: Perceived privacy of photo-based memes

Study 1 participants completed a task assessing their interdependent privacy perceptions, or the extent to which they perceived photo-based memes depicting strangers as private, in addition to completing questionnaires. We elaborate on this method next.

3.3.1 Participants

Participants were recruited via Amazon's Mechanical Turk online recruitment system. To be eligible for our study, participants had to be living in the United States, fluent in English, between the ages of 18 and 60, and regular social media users (i.e., have an active social media account that they visit at least once per week). To improve the quality of data collection on MTurk, we required that respondents have completed at least 100 tasks on the website with at least 98% success rate prior to signing up for the survey, meaning that participants had a history of providing reliable responses. Several additional steps were then taken to ensure participants completed the survey attentively and honestly. We excluded participants who provided nonsensical responses to open-ended questions (i.e., providing incoherent responses that did not address the question or answers that were copied from the internet), and excluded those who selected the same response item across multiple forms (e.g.., selecting only "B" to multiple questionnaires). As an added attention check, we also presented two duplicate questions regarding the participant's age and the social media platforms they used, and participants were excluded if they provided contradictory responses to either item (i.e., by reporting their age inconsistently or by indicating they did not use social media in one instance while selecting multiple platforms in the other). Finally, we removed participants who completed the survey in under 10 minutes, which was determined to be unreasonably fast based on pilot data. Two participants were removed due to non-completion, 28 for non-sensical responses, four for providing overly uniform responses, nine for failing the in-survey attention checks, and 16 for unreasonably fast completion times. An additional 11 participants were excluded for violating multiple of the above conditions. Our final sample consisted of 245 respondents after applying our exclusion criteria, with an average age of 34.21 years (SD = 9.40). The majority of participants identified as male (61.63%), while 38.37% identified as female. In terms of racial composition, 53.06% of participants identified as White, 21.22% as Asian, 11.02% as Hispanic/Latinx, 6.53% as biracial or multiracial, 5.71% as Black or African-American, 2.04% as American Indian or Alaska Native, and 0.41% as "Other". Most participants held a bachelor's degree (44.90%), followed by 24.49% with a graduate degree, 15.92% with a high school diploma or equivalent, 14.29% having earned an associate degree, and 0.41% having completed some college. Participants had an average of 4.21 social media accounts (SD = 1.69) and reported sharing photos on an average of 2.14 accounts (SD = 1.23). Table 2 provides a summary of social media platforms used by participants.

Table 2: Percentage of participants with an account and who share photos per social media platform. *Other platforms include Minds, Parler, Discord, Odyssey, Linkedin, WhatApp, BitChute, Youtube, and Myspace.

Name of platform	Percentage with account	Percentage who share photos
Facebook	91.84 %	76.33 %
Instagram	82.04 %	60.00 %
Twitter	77.14 %	38.37 %
Snapchat	31.02 %	14.69 %
Reddit	27.76 %	10.61 %
TikTok	26.53 %	8.57 %
Pinterest	27.75 %	4.08 %
Flickr	4.49 %	0.82 %
Other*	3.67 %	0.41 %

3.3.2 Procedure

All study procedures were approved by our Institutional Review Board for the conduct of human subject research. After providing informed consent, participants were asked to complete the Social Media Usage Questionnaire. Next, participants completed the privacy perception task where they provided privacy ratings of the 68 memes described above in random order. Prior to viewing the memes, participants were provided with the following instructions: "Next you will view a series of memes modified from real social media posts. As you view the memes, please imagine that you are navigating your own social media account and indicate how likely you would be to share or re-share the meme on social media." They were then presented with each image separately and rated their level of agreement with the following statement: "It is too private to share on social media." Responses were recorded using a five-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree). Some of the memes rated by participants contained content that may be considered offensive, and participants were warned about this content during consent and prior to completing the task so that they had multiple opportunities to opt out. Finally, participants completed the remaining self-report questionnaires (§ 3.2) and provided demographic information.

3.4 Study 2: Coding of perceived meme entertainment, shareability, and valence

We conducted Study 2 as a follow-up to our initial data collection to code for the perceived valence, likelihood of sharing on social media, and entertainment value of the 68 images presented during the privacy perception task in Study 1. This allowed us to investigate the relationship between perceived privacy and sharing likelihood, as well as potential moderating factors such as entertainment value and valence. Taken together, Studies 1 and 2 also allowed us to investigate the interplay between meme and user characteristics in determining privacy perceptions.

3.4.1 Participants

Participants were recruited from Amazon's Mechanical Turk platform using the same eligibility requirements described previously and were randomly assigned to one of three rating conditions (i.e., rating either the sharing likelihood, valence, or entertainment value of each image). After screening for ineligible responses, 29 participants were removed for providing nonsensical response to open-ended questions, two for providing overly uniform responses (i.e., "one-lining"), 45 for failing the in-survey attention checks, and 12 for unreasonably fast completion times. An additional 16 were excluded for violating multiple of the above conditions. The final sample included 111 participants in the sharing likelihood condition, 104 in the valence condition, and 145 in the entertainment condition. The average age of participants was 35.37 (*SD* = 9.60*)*, 35.49 (*SD* = 9.60*)*, and 37.49 (*SD* = 9.82*)* respectively. There were also more male than female participants in each of the three conditions (61.26% vs. 37.84% who rated sharing likelihood, 60.58% vs. 38.46% who rated valence, and 62.76% vs. 35.86% who rated entertainment). In addition, 0.90% of participants in the sharing likelihood condition and 0.69% in the entertainment condition identified as non-binary/third gender, while 0.96% of participants in the valence condition and another 0.69% in the entertainment condition chose not to disclose their gender.

In terms of racial composition, most participants in the sharing likelihood condition identified as White (72.97%), while 9.01% identified as Asian, 5.41% as Black or African-American, 3.60% as American Indian or Alaska Native, 2.70% as Hispanic/Latinx, and 6.31% as biracial or multiracial. Similarly, participants who completed the valence rating task were also majority White (60.58%), followed by Asian (18.27%), Black or African American (6.73%), American Indian or Alaska Native (6.73%), Hispanic/Latinx (1.92%), and biracial or multiracial (5.77%). Finally, participants who completed the entertainment ratings were mostly White (70.24%), followed by Asian (10.34%), Hispanic/Latinx (6.90%), Black or African-American (4.83%), American Indian or Alaska Native (2.76%), and biracial/multiracial (4.83%). The educational level of participants ranged from graduate degrees to high school diploma or equivalency, with the largest group across all three studies consisting of college graduates with a bachelor's degree (54.95%, 55.77%, and 48.97% in the sharing likelihood, valence, and entertainment value conditions respectively).

3.4.2 Stimuli and experimental manipulation

Participants rated the same 68 social media images presented during the privacy perception task in Study 1. These images were presented in random order at the top-center of the participant's screen. In the sharing likelihood condition, participants responded to the question "How likely are you to share or re-share this post on social media?" on a five-point Likert scale from 1 (*Extremely Unlikely*) to *5* (*Extremely Likely*). Likewise, participants in the valence condition rated the valence of each meme ("To what extent does this post portray the person in the photo negatively or positively?") on a Likert scale from 1 (*Very Negatively*) to *5* (*Very Positively*). Finally, participants in the entertainment condition rated the entertainment value of each meme by responding to the question "How funny or entertaining do you find this post?" on a scale from 1 (*Not at all funny/entertaining"*) to 5 (*Very funny/entertaining"*). After rating the stimuli, participants provided the same demographics information as collected in Study 1.

4 RESULTS

4.1 Preliminaries

Study 1 participants completed a privacy perception task where they viewed a series of social media memes and rated the degree of private content presented in each. The average privacy rating across memes was 2.90 (*SD* = .50) out of 5, with higher ratings indicating that the meme was perceived as more private. Study 2 participants who rated the memes on additional characteristics indicated an average entertainment value of 3.18 *(SD* = .45), sharing likelihood of 2.72 *(SD* = .38), and valence of 3.06 *(SD* = .86).

Because this project focuses on factors influencing interdependent privacy perceptions, the analyses presented hereon refer to participants who rated memes on perceived privacy, unless stated otherwise. Average meme ratings of entertainment, sharing likelihood, and valence obtained from participant groups are included as independent variables in several statistical models below.

Most participants indicated that they shared online photos multiple times a week (31%), followed by multiple times a month (22%), once a week (14%), multiple times per day (11%), less than once per month (9%), and never (3%). The most frequent target audience for photo sharing was friends (47%), followed by friends and public viewers (40%), and public viewers (11%), while 2% of participants indicated they did not share photos. Finally, the average score on the SMD was 2.32 (*SD* = 1.13) out of five, with higher scores representing a greater degree of problematic social media behaviors. Scores on the SMD were highly correlated with age (*r* (243) = -.51, *p* < .001), socioeconomic status (*r* (243) = .69, *p* <.001), and scores on the SD3 (*r* (243) = .74, *p* < .001). Given that DT and LT dimensions of the SD3 questionnaire were of primary interest, SMD was excluded from further analysis.

4.1.1 Education, race, and socioeconomic status predict interdependent privacy perceptions

We used a series of linear regression and mixed-effects models to compare perceived meme privacy to user characteristics including demographics, personality traits, and social media usage behaviors. For the following linear regression models, the privacy ratings of the 68 memes presented during the image rating task were averaged into a single continuous score per participant and included as the dependent variable in each analysis. There is debate over the application of parametric models to Likert scale data; however, our approach is consistent with recent recommendations in the literature [38]. Finally, a variance inflation factor (VIF) of 4 was included as a cutoff when evaluating fit [1].

As a part of our preliminary analysis, we investigated how user demographics and social media usage contributed to interdependent privacy perceptions. First, we fit a linear regression model with each participant's average privacy rating as the outcome variable and demographic information as predictors (see Table 3). The reference levels for the race and gender variables were set to the categories with the highest number of observations. We found several significant effects of demographics on privacy perceptions (R^2= .52, *F* (11, 233) = 22.45, *p* < .001). Participants who identified as White rated the memes as less private on average than participants who identified as Asian (*β* = .46, *p* < .001) or Hispanic (*β* = .57, *p* = .001). Education was also a significant predictor of privacy ratings, and users with an associate (*β* = .77, *p* < .001), bachelor (*β* = .47, *p* = .001), or graduate degree (*β* = .63, *p* < .001) rated the memes as more private on average than participants whose highest degree earned was high school or equivalent. Lastly, socioeconomic status (SES) was positively related to privacy ratings (*β* = .42, *p* < .001), such that participants identifying as higher SES also rated memes as relatively private, but the effects of age (*p* = .09) and gender (*p* = .77) were not statistically significant. We discuss these relationships further in § 5.

Table 3: Standardized estimates (*β*) for linear regression model examining the relationship between participant demographics and interdependent privacy perceptions.

	Average Privacy Rating		
Predictors	*β*	*CI*	*p*
Intercept	-.64	-.90 – -.38	**<.001**
Age	-.09	-.19 – .01	.09
SES	.42	.30 – .53	**<.001**
Race: [White]	*Reference*		
Race: [American Indian or Alaska Native]	.61	-.04 – 1.26	.07
Race: [Asian]	.46	.21 – .71	**<.001**
Race: [Biracial/Multiracial]	-.35	-.74 – .04	.08
Race: [Black or African American]	.04	-.37 – .45	.86
Race: [Hispanic/Latinx]	.57	.22 – .92	**.001**
Gender: [Male]	*Reference*		
Gender: [Female]	.03	-.16 – .22	.77
Education: [High school or equivalent]	*Reference*		
Education: [Associate degree]	.77	.43 – 1.10	**<.001**
Education: [Bachelor's degree]	.47	.18 – .75	**.001**
Education: [Graduate degree]	.63	.30 – .97	**<.001**
Observations		245	
R^2 / R^2 adjusted		.52 / .49	

4.1.2 Interdependent privacy perceptions are associated with higher frequency and variety of social media usage

The last of the preliminary analyses included a linear regression to examine the relationship between interdependent privacy perceptions and self-reported social media usage behaviors. Participants' average privacy ratings were included as the outcome variable with total number of social media accounts, photo-sharing frequency, social media visit frequency, and photo sharing preference (i.e., whether they share their own photos more compared to photos of other people) as predictors (see Table 4). Participants who reported sharing photos more frequently (β = .36, p < .001) and those who reported sharing their own photos more often than they shared other people's photos (β = .42, p = .001) rated the memes as more private. However, there was a significant negative relationship between social media visit frequency (β = -.35, p < .001) and total number of accounts (β = -.17, p = .004) with privacy ratings.

Table 4: Standardized estimates (β) for linear regression model examining the relationship between social media usage and interdependent privacy perceptions.

	Average Privacy Rating		
Predictors	*β*	*CI*	*p*
Intercept	-.34	-.53 – -.16	<**.001**
Number of Social Media Accounts	-.17	-.28 – -.06	**.004**
Photo Sharing Frequency	.36	.24 – .49	<**.001**
Sharing Preference: [I share others' photos more]	*Reference*		
Sharing Preference: [I share and re-share equally]	.66	.37 – .95	<**.001**
Sharing Preference: [I share my own photos more]	.42	.17 – .67	**.001**
Sharing Preference: [I do not share photos]	.33	-.48 – 1.15	.42
Social Media Visit Frequency	-.35	-.46 – -.23	<**.001**
Observations	245		
R^2 / R^2 adjusted	.31 / .30		

4.2 Relationship between interdependent privacy perception and sharing likelihood is moderated by meme entertainment value

To investigate how user perceptions of privacy were related to other subjective qualities of the memes, we averaged participants' ratings by meme so that each meme in the dataset (n = 68) had an aggregated value for privacy, valence, entertainment value, and sharing likelihood, as rated by independent participant groups. We then fit a linear regression model with average privacy rating as the outcome variable and average valence, entertainment value, and sharing likelihood as predictors (see Table 5). We also included a three-way interaction term to assess how the affective qualities of the meme (i.e., entertainment value and valence) interacted with users' willingness to share the meme on social media. We found a significant negative relationship between sharing likelihood and privacy (β = -.58, p < .001), indicating that memes perceived as more private were rated by social media users as less shareable. However, this relationship was moderated by entertainment value (β = .29, p = .01), such that the relationship between sharing likelihood and privacy was significantly diminished when the memes were perceived as entertaining (see Figure 1). Taken together, entertainment value, sharing likelihood, and valence explained 51% of the variance in average privacy ratings (F (7, 60) = 8.94, p < .001), constituting a medium to large effect size [27].

Table 5: Standardized estimates (β) for linear regression model examining the relationship between meme entertainment, shareability, and valence and interdependent privacy perceptions.

	Average Privacy Rating		
Predictors	*β*	*CI*	*p*
Intercept	-.11	-.35 – .13	.38
Entertainment Value	-.09	-.36 – .18	.50
Sharing Likelihood	-.58	-.89 – -.27	**<.001**
Valence (Negative to Positive)	.11	-.17 – .39	.44
Entertainment * Sharing Likelihood	.29	.09 – .50	**.01**
Entertainment * Valence	-.05	-.33 – .23	.71
Valence * Sharing Likelihood	-.09	-.30 – .13	.43
Entertainment * Valence * Sharing Likelihood	.04	-.16 – .25	.69
Observations		68	
R^2 / R^2 adjusted		.51 / .45	

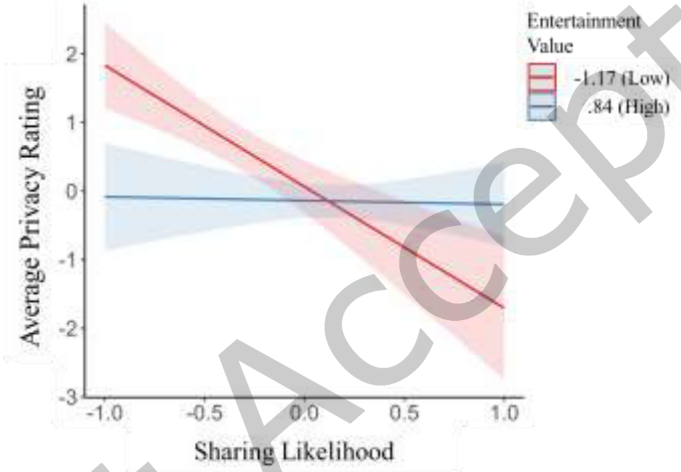

Figure 1: Interaction effect of meme shareability and entertainment value on average privacy ratings. Sharing likelihood is higher when memes are rated as less private, assuming the meme has low entertainment value (red line). However, when the meme is highly entertaining (blue line), the relationship between sharing likelihood and privacy ratings is eliminated.

4.3 Big five, DT, and LT personality traits are associated with heightened interdependent privacy perceptions

In order to examine the relationship between personality traits and privacy perceptions, we entered participants' average privacy ratings into a linear regression model as the outcome variable with subscales from the BFI-10, LTS, and SD3 as predictors, along with self-reported personal privacy preference (see Table 6). We found that the agreeableness (β = -.14, p = .04) and openness (β = -.19, p < .001) subscales of the BFI-10 were negatively related to privacy ratings, while the conscientiousness, extraversion, and neuroticism subscales were not significantly related (ps > .05). In addition, we found that faith in humanity (β = .31, p < .001) and psychopathy (β = .31, p < .001) personality traits of the LT and DT scales were associated with heightened interdependent privacy ratings. Overall, individual differences in personality traits provided a strong prediction of interdependent privacy perceptions, explaining 56% of the variance (R^2= .56, F (12, 232) = 24.73, p < .001).

The finding that both faith in humanity and psychopathy were positively related to privacy perceptions was somewhat surprising considering that the DT and LT were developed to measure opposing personality traits (i.e., maladaptive versus adaptive traits) [57]. However, a follow-up exploratory correlation analysis revealed that overall DT scores did not significantly correlate with LT scores, r (243) = -.09, p = .166. In fact, Kantianism was the only LT trait negatively correlated with the DT, r (243) = -.38, p < .001, while narcissism was positively correlated with both faith in humanity, r (243) = .25, p < .001, and humanism, r (243) = .23, p < .001. Thus, we found evidence that DT and LT personality traits do not represent mutually opposing characteristics, aligning with previous LT research [69].

Table 6: Standardized estimates (*β)* for linear regression model examining the relationship between BFI-10, DT, and LT personality traits and interdependent privacy perceptions.

	Average Privacy Rating		
Predictors	*β*	*CI*	*p*
Intercept	.00	-.09 – .09	**<.001**
BFI-10: [Extraversion]	-.11	-.23 – .01	.07
BFI-10: [Agreeableness]	-.14	-.27 – -.00	**.04**
BFI-10: [Conscientiousness]	-.07	-.19 – .06	.31
1BFI-10: [Neuroticism]	.04	-.07 – .16	0.50
BFI-10: [Openness]	-.19	-.29 – -.09	**<.001**
Privacy Preference Question	.15	.04 – .26	**.01**
SD3: [Machiavellianism]	.06	-.08 – .20	.50
SD3: [Narcissism]	.10	-.04 – .23	.16
SD3: [Psychopathy]	.31	.15 – .46	**<.001**
LTS: [Humanity]	.31	.16 – .46	**<.001**
LTS: [Humanism]	.08	-.04 – .21	.19
LTS: [Kantianism]	.07	-.04 – .17	.20
Observations		245	
R^2 / R^2 adjusted		.56 / .54	

4.4 Psychopathic personality is associated with increased privacy ratings and photo sharing of strangers

Given that the psychopathy subscale of the DT is associated with impulsivity and a lack of empathy [18,52,70], the positive relationship between psychopathy and interdependent privacy ratings was contrary to our hypothesis that DT users would rate photo-based memes as less private than others. Based on the DT findings in the previous model, we developed a hypothesis that narcissism and psychopathy taken together would provide additional insights into the paradoxical finding that high-DT users exhibited heightened interdependent privacy perceptions. Specifically, because previous research indicates that narcissism is associated with the maintenance of positive self-image on social media [29,74,95], we hypothesized that users high in psychopathy *and* narcissism would be motivated to express a type of moral superiority by reporting memes as private despite sharing such content online themselves. Thus, we repeated the previous model with an additional term to describe the interaction between narcissism and psychopathy. We found that narcissism moderated the effect between psychopathy and privacy perception (β = .12, p = .03), such that the relationship between psychopathy and privacy ratings was significantly diminished when participants scored low on narcissism (see Figure 2).

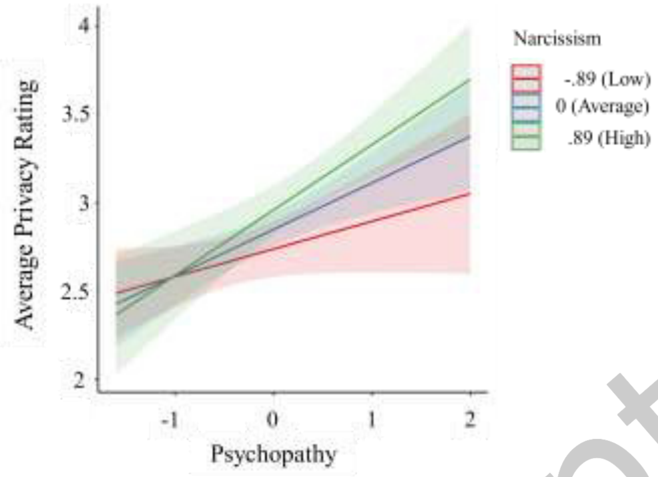

Figure 2: Interaction effect of DT psychopathy and narcissism on average privacy ratings. Users high in psychopathy tend to rate photo-based memes as more private. This effect is amplified among users who are high in narcissism (green line) versus low in narcissism (red line).

Next, following the finding that high-DT users rated memes as more private, we sought to confirm our hypothesis that high-DT users would report sharing more photos of themselves and other people online—a finding that would be in line with prior work indicating increased self-disclosure and selfie sharing by DT personality types [74,95,96]. We regressed the frequency of two types of photo sharing (i.e., photo sharing of friends or family versus photo sharing of strangers) on the three DT subscales. We also included total photo sharing frequency as a covariate in these models to control for differences in overall sharing behaviors. We found that psychopathy positively predicted photo sharing of strangers (β = .16, p = .008), whereas narcissism positively predicted photo sharing of friends, family, or self (β = .17, p < .001). We found no other significant relationships between DT traits and photo sharing frequency, p > .05.

Finally, the finding that high-DT users rated memes as private and shared photos of other people frequently appeared to contradict our first model, which showed a strong negative correlation between meme privacy and shareability ratings. We sought to untangle this relationship further by conducting a follow-up mixed-effects model to examine how DT scores interacted with each meme's shareability and entertainment value. We included users' individual privacy ratings of the 68 social media memes as the outcome, total SD3 score as the predictor to reflect overall DT characteristics, and participant ID as the random intercept (see Table 7). We also included terms describing the interactions between users' overall DT characteristics and each meme's average entertainment value and sharing likelihood. As suspected, we found a significant three-way interaction between scores on the SD3, entertainment value, and sharing likelihood (β = -.43, p < .001). There was a noticeable dissociation between sharing likelihood and privacy ratings when memes were rated by high-DT users (see Figure 3), and this interaction was further moderated by the entertainment value of the meme. Although this does not include a direct measurement of intentional privacy violations, the disconnect between privacy ratings and shareability suggest that users high in DT personality traits shared memes despite understanding the sensitivity of their content, and this effect was particularly strong for highly entertaining memes. In other words, high-DT users were more likely to disregard interdependent privacy when memes were entertaining.

Table 7: Mixed-effects model examining the interaction between DT, entertainment value, and meme shareability.

		Privacy Rating	
Predictors	*Estimates*	*CI*	*p*
Intercept	2.83	2.73 – 2.92	**<.001**
Entertainment Value	-.10	-.14 – -.05	**<.001**
Sharing Likelihood	-.67	-.72 – -.61	**<.001**
Dark Triad	.66	.54 – .77	**<.001**
Entertainment Value * Sharing Likelihood	.72	.62 – .81	**<.001**
Entertainment Value * Dark Triad	-.08	-.14 – -.02	**.006**
Sharing Likelihood * Dark Triad	.77	.71 – .84	**<.001**
Entertainment * Sharing Likelihood * Dark Triad	-.43	-.55 – -.31	**<.001**
Random Effects			
σ^2		1.12	
$\tau_{00\ \text{ResponseId}}$		.51	
ICC		.31	
$N_{\text{ResponseId}}$		245	
Observations		16660	
Marginal R^2 / Conditional R^2		.20 / .45	

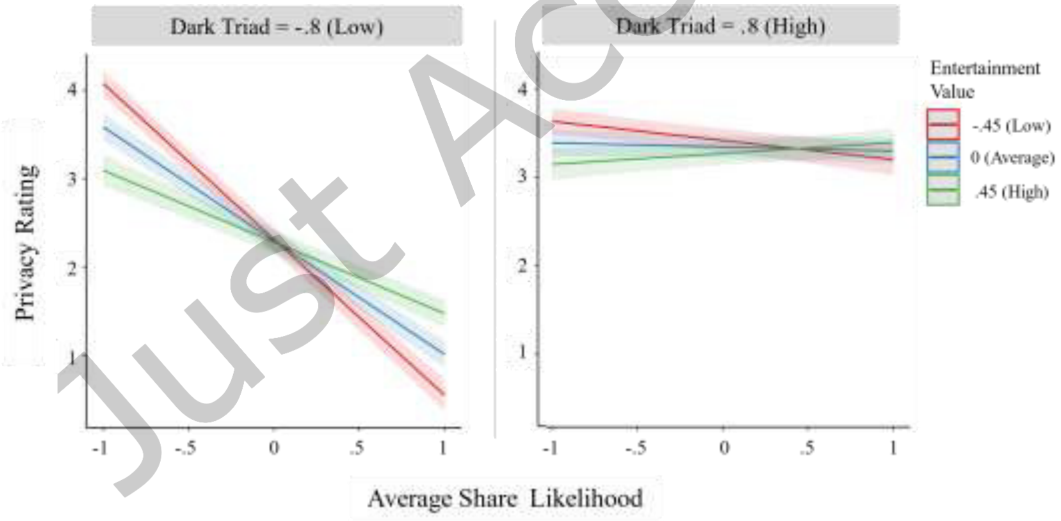

Figure 3. Three-way interaction effect of overall DT score, meme shareability, and meme entertainment value on average privacy ratings. Low-DT participants (left panel) share less when memes are perceived as private, though this relationship is weakened when memes are highly entertaining (green line) versus low entertaining (red line). In contrast, high-DT participants (right panel) do not show a strong relationship between a sharing likelihood and privacy ratings.

4.5 Interdependent privacy perceptions vary among distinct user types

In addition to examining user characteristics associated with interdependent privacy perceptions, a second primary objective of the study was to identify clusters of users with distinct interdependent privacy attitudes and behaviors. We used k-prototypes clustering [45,106] to partition users based on the variables that were identified above as relevant to interdependent privacy, including education, SES, social media usage, personality traits, and privacy preference, with lower scores representing a stronger preference for privacy. The k-prototypes algorithm was developed as an extension to k-means to allow for the use of mixed-type data [45]. Based on a silhouette approach [56], the optimal number of clusters was determined to be three, and the algorithm was configured with 25 random initializations.

Examining descriptive statistics to characterize the traits of users in each cluster (see Table 8), we found that cluster 3 participants were the youngest (*M* = 29.63, *SD* = 8.08), reported the highest SES (*M* = 7.89, *SD* = .89), and were the most frequent sharers of photos containing friends and family (*M* = 4.51, *SD* = 1.57) as well as photos of strangers (*M* = 4.22, *SD* = 1.86). Cluster 3 participants also reported the highest average Machiavellianism (*M* = 3.86, *SD* = .65), narcissism (*M* = 3.38, *SD* = .49), and psychopathy (*M* = 3.26, *SD* = .66) personality traits. Considering cluster 3 participants had both the highest average privacy ratings (*M* = 3.66, *SD* = .72) and DT personality scores, this partitioning was consistent with the previously reported positive relationship between DT personality and privacy perceptions. Taken together, we theorized that this group of users was composed of 'privacy violators.' In other words, these participants demonstrated an awareness of interdependent privacy, frequently shared photos of other people despite having that awareness and had personality traits consistent with impulsivity and a lack of empathy.

Similarly, we characterized cluster 2 participants as 'privacy ignorers.' Although these users frequently shared photos on social media (*M* = 4.72, *SD* = 1.30), they rated the memes as less private (*M* = 2.43, *SD* = .59) than those in cluster 3. We suspected that cluster 2 was composed of participants who shared images of other people but had an overall lack of awareness of interdependent privacy. Finally, participants in cluster 1 were considered 'privacy preservers' as they were relatively infrequent image sharers (*M* = 2.09, *SD* = 1.24) and reported a strong preference for maintaining personal privacy (*M* = 3.02, *SD* = 1.46). Cluster 1 users appeared to be older (*M* = 37.05, *SD* = 10.00), scored low on DT personality traits, and perceived memes as less private than those in cluster 3.

Table 8: Average privacy ratings, demographics features, social media usage, and personality traits per cluster. Bolded items were included in the k-prototype algorithm when identifying clusters. Un-bolded items are included for additional description of the user clusters.

	Cluster 1	**Cluster 2**	**Cluster 3**
	Privacy Preservers	Privacy Ignorers	Privacy Violators
	M (SD)	*M (SD)*	*M (SD)*
Privacy Rating	2.50 (.66)	2.43 (.59)	3.66 (.72)
Age	37.05 (10.00)	36.75 (8.55)	29.63 (8.08)
Privacy Preference Questionnaire	3.02 (1.46)	3.18 (1.41)	5.14 (1.44)
Social Media Visit Frequency	6.29 (.97)	6.82 (.52)	5.70 (1.75)
SES	4.22 (1.50)	4.64 (1.36)	7.89 (.89)
Photo Sharing Frequency	-	-	-
Overall	2.09 (1.24)	4.72 (1.30)	4.73 (1.65)
Friend, Family, or Self	1.93 (1.23)	3.70 (1.64)	4.51 (1.57)
Neither Friend nor Family	1.66 (1.32)	3.90 (1.72)	4.22 (1.86)
Big-Five Personality	-	-	-
Agreeableness	3.21 (1.08)	3.74 (1.04)	3.28 (.81)
Conscientiousness	4.17 (.81)	4.18 (.98)	3.47 (.79)
Extraversion	2.57 (1.14)	2.63 (1.21)	3.11 (.71)
Openness	3.61 (1.03)	3.73 (1.07)	3.05 (.67)
Neuroticism	2.72 (1.12)	2.44 (1.27)	2.73 (.76)
Dark Triad	-	-	-
Machiavellianism	2.87 (.94)	2.94 (.90)	3.86 (.65)
Narcissism	2.28 (.87)	2.51 (.88)	3.38 (.49)
Psychopathy	2.00 (.80)	1.87 (.72)	3.26 (.66)
Light Triad	-	-	-
Faith in Humanity	3.16 (1.06)	3.49 (1.05)	4.12 (.57)
Humanism	3.63 (.91)	3.99 (.79)	4.20 (.50)
Kantianism	4.19 (.74)	4.12 (.80)	4.07 (.48)
Cluster Size (*n*)	*n* = 59	*n* = 96	*n* = 90

5 DISCUSSION

Social media has given rise to large-scale interdependent privacy issues, but little is known about how individual differences in user characteristics contribute to sharing decisions. In order to effectively influence users, interventions promoting privacy preservation require greater precision in targeting users based on their underlying motivations and privacy preferences. The objective of the present study was to identify key user characteristics associated with interdependent privacy perceptions, including user demographics, personality dimensions, and social media activity. We also examined how additional perceptions of the photo-based memes—entertainment value, shareability, and valence—covaried with privacy perceptions. In doing so, we identified strong predictors of interdependent privacy perceptions and established three primary user types who differ in their interdependent privacy preferences.

5.1 Linkages between interdependent privacy perceptions and sharing on social media

An important question in the interdependent privacy literature concerns how privacy perceptions relate to sharing decisions, as well as how this relationship is moderated by social motivations for sharing decisions, including: 1) entertainment value (i.e., potential for entertaining social media connections); and 2) valence (i.e., potential for damaging the photo subject's reputation). A series of studies by Amon and colleagues [3] demonstrated that, in general, negatively valenced photo-based memes were shared less by users, but prompts reminding users to consider the meme subject's privacy consistently backfired to increase the sharing of other people's photos. Because the latter finding suggests that shareability and privacy saliency can be anticorrelated, we hypothesized that privacy perceptions and sharing likelihood ratings of photo-based memes would not be strongly related.

Inconsistent with this hypothesis, we found that memes perceived as more private were also rated as less shareable, suggesting participants generally believed it would be inappropriate to share private content of other people. However, this relationship depended significantly on the perceived entertainment value of the meme, such that there was a marked dissociation between privacy perceptions and sharing likelihood when the meme was highly entertaining. This finding suggests that users balance the benefits of sharing socially desirable memes against the costs of violating user privacy. When memes are highly entertaining, users seem to suppress their privacy concerns, possibly because the motivation to share has overtaken the concern for privacy. Conversely, when entertainment value is low, there is little motivation to share memes that could be received poorly by other users due to their sensitive content.

Memes are generally shared with the intention of being entertaining, and our findings are consistent with literature reporting that humor is related to the willingness to share private photos on social media [40]. Furthermore, while we focus on entertainment and valence due to the nature of viral memes, research on multiparty privacy suggests there are several additional image characteristics relevant to sharing decisions. Specifically, when investigating privacy concerns regarding co-owned images (i.e., group photos), perceived image privacy appears to depend on the number of people in the photo [43], the intended audience [105,118], and the sensitivity of disclosed information [66]. Together, our findings lend further support to the privacy calculus model [65] by demonstrating how users weigh out the pros and cons of sharing an image to their social media profile, sometimes to the detriment of interdependent privacy.

5.2 Contribution of Dark Triad personality traits to interdependent privacy literature

When analyzing the relationship between dark triad personality and privacy preferences, we found mixed support for our hypotheses. The results of our linear regression models and cluster analysis support our initial prediction that high-DT users would report more frequently sharing photos of themselves and strangers. However, we also uncovered a somewhat counterintuitive finding that those high in psychopathy rated photo-based memes as more private than other users. That is, it might be assumed that those with an interest in privacy preservation (i.e., those who share less than others online and are low in DT) would perceive potentially sensitive photo-based memes of strangers as relatively private. However, our finding that psychopathy is positively related to privacy ratings conflicts with this assumption, especially because psychopathy was tied to self-reports of higher photo sharing online of strangers. Thus, our results did not support our third hypothesis predicting reduced privacy perceptions by high-DT users.

There are three primary explanations for the finding that high-DT users rate photo-based memes as more private than others. First, given that high-DT users are more likely to engage in trolling, cyberbullying, and other intrusive acts toward others (esp. psychopathic users; see § 2.2) [5,32,34,94], high-DT users may be particularly motivated to attune to others' privacy as they actively seek to manipulate others. Second, high-DT users may also have more experience in posting and viewing potentially sensitive content than other users, providing them with opportunities to learn what people consider private. In addition to sharing more photos of close connections and strangers, high-DT users report problematically high social media usage [16,19,58], meaning that these users may be exceptionally familiar with viewing people's reactions to private material online. Third, it is possible that participants with dark triad personality rated the memes as 'too private to share' to present a positive image of their attitudes even though those attitudes were not reflected by their actual social media behaviors. That is, high-DT users have been shown to carefully curate their online presence in an effort to present a more positive image of themselves and are motivated by a need for self-enhancement (esp. narcissistic users) [12,29,74,76,92,95]. The definition of self-enhancement as an 'unrealistically positive self-view' [22] is consistent with high-DT users attempting to express a type of moral superiority by identifying memes as private while also reporting they often share such content online.

5.3 Dark Triad subdimensions associated with interdependent privacy perceptions

Our findings that high-DT users shared more memes and rated them as more private than others appeared to contradict our first model that highlighted a strong negative relationship between privacy perceptions and shareability ratings. Thus, we conducted follow-up analyses examining the relationships between narcissism, psychopathy, and photo sharing frequency. We show that narcissism significantly interacts with psychopathy to predict privacy perceptions, such that privacy ratings of memes were highest when rated by individuals with both narcissism *and* psychopathy personality traits. However, the relationship between privacy ratings and psychopathy was diminished when participants reported low trait narcissism. This supports the idea that users with a psychopathic personality, driven by co-occurring narcissism, rate memes as private to present an inflated representation of their beliefs. Furthermore, we show that the underlying behaviors of users with psychopathy personality are in direct conflict with their inflated privacy ratings. Not only do users high in psychopathy more frequently share photos of strangers, but high-DT users are more likely to disregard privacy in favor of entertainment. The follow-up analyses clarify the relationship between dark triad personality and privacy perceptions, indicating that DT personality types may intentionally violate interdependent privacy despite their acute understanding of privacy norms. Finally, we also show that narcissism is uniquely associated with increased sharing of photos containing family, friends, or self, confirming previous literature linking narcissism to increased self-disclosure behaviors [29,74,95,96]. There appears to be a complex relationship between personality and sharing behaviors, and our analyses highlight how attention seeking and antisocial personality traits interact and contribute to maladapted interdependent privacy attitudes.

5.4 Light Triad and Big Five dimensions associated with interdependent privacy perceptions

In addition to exploring the contributions of maladaptive DT personality traits, we also investigated the influence of adaptive LT personality traits, finding that faith in humanity was associated with heightened interdependent privacy perceptions. Higher scores on the faith in humanity subscale represent a general belief in the goodness of other people, and LT personality is more broadly related to compassion and empathy [57]. Limited research has linked LT personality to prosocial online behaviors [72], but our work is the first to investigate the relationship between LT personality and online privacy behaviors. Given the linkage between LT personality and empathy [57], perhaps individuals who have high regard for others also have a greater empathic concern for their interdependent privacy.

In terms of the Big Five personality dimensions, higher levels of user agreeableness and openness predicted reduced privacy perceptions. These traits are associated with increased trust [25,33] and open-mindedness [35], which may, in turn, make people less cautious and more trusting of other users, including in the context of social media sharing. Junglas and colleagues [54] support this hypothesis by showing reduced concern for personal privacy in individuals who are agreeable and open; however, research on the topic is inconsistent [81,101]. In this case, higher agreeableness and open-mindedness may encourage users to view the frequency of photo-based memes on social media with acceptance, versus questioning the status quo. Notably, our findings do not intersect with literature linking low agreeableness, high extraversion, and high neuroticism to cyberbullying [5,17,28,31]. Our findings support the notion that photo-based memes are shared primarily for reasons of entertainment, which may not be the motivation behind cyberbullying. For this reason, the user characteristics that drive cyberbullying versus sharing of photo-based memes may differ to some degree.

5.5 Interdependent privacy user categories

Leveraging key insights from our regression models, we entered variables significantly associated with interdependent privacy perceptions into a cluster analysis, which yielded three distinct interdependent privacy user categories (IPUC) that we label as “privacy preservers”, “privacy ignorers”, and “privacy violators” (see Figure 4). Privacy preservers included those who refrained from sharing photos on social media regardless of their privacy perceptions. Individuals belonging to this user type reported the lowest frequency of photo sharing across all photo types (friends, family, or strangers) and the strongest preference for maintaining personal privacy. Their infrequent photo sharing and strong preference for privacy suggests that they are acting to preserve privacy (their own and that of others) by limiting information disclosure. On the other hand, privacy ignorers included those who shared photos at a high rate but did not perceive photo-based memes depicting strangers as too private for social media. These users tended to be older, low-DT personalities with lower levels of education and SES. Given their high rate of photo sharing and reduced privacy perceptions, these users may be unaware of interdependent privacy when making sharing decisions, perhaps due to a lack of privacy literacy. This was in direct contrast to privacy violators, who both reported sharing photos of strangers frequently and acknowledged that photos depicting strangers were ‘too private to share.’ These "privacy violators” may have been strongly motivated by their DT personality traits, as these users scored highest across all three DT subscales. This user type was also the youngest with noticeably higher levels of SES, education, and photo-sharing frequency. Considering the relationships between personality and photo sharing discussed above, we suspect that these users have a large amount of experience with photo sharing and that they are knowingly violating interdependent privacy in favor of sharing entertaining memes.

Our IPUC model overlaps to some degree with Westin’s [115] characterization of consumers as privacy fundamentalists, privacy unconcerned, and privacy pragmatists. The overlap is notable given that Westin’s model centers on consumer preferences for one's own privacy, whereas our model focuses on attitudes and behaviors towards other people's privacy on social media. Westin's privacy fundamentalists and the present category "privacy preservers" appear to recognize privacy risks and err on the side of caution by sharing less information. Both Westin's privacy unconcerned and our "privacy ignorers" emphasize the benefits of sharing over the risks. The models deviate when it comes to comparing Westin's privacy pragmatists to our "privacy violators." Westin identifies privacy pragmatists as those who make informed and rational decisions as they negotiate their privacy within the marketplace. Similarly, our "privacy violators" are informed in reporting a relatively high degree of interdependent privacy awareness and consider the entertainment value of content when making privacy decisions—weighing the pros and cons of sharing to make privacy decisions. However, our model highlights user motivations behind potentially harmful behaviors toward others. In the case of privacy violators, they cannot be characterized as especially rational. In fact, their recognition of negative sharing consequences (i.e., harm toward others) is inconsistent with their sharing behaviors.

Overall, the IPUC model findings of three distinct user types that vary in interdependent privacy attitudes and behaviors suggests the need for more targeted intervention strategies. That is, our model suggests that interdependent privacy literacy or educational strategies are unlikely to be effective in reducing breaches from "privacy violators," or those who are high in dark triad characteristics and regularly share others' information despite exhibiting heightened awareness of others' privacy. Instead, privacy violators may be more influenced by disincentives, for example, where their ability to interact with others is limited based on their participating in harmful activities. On the other hand, privacy literacy interventions may be especially valuable for users in the "privacy ignorer" category who appear to share others' information without exhibiting awareness of the potential for interdependent privacy violations.

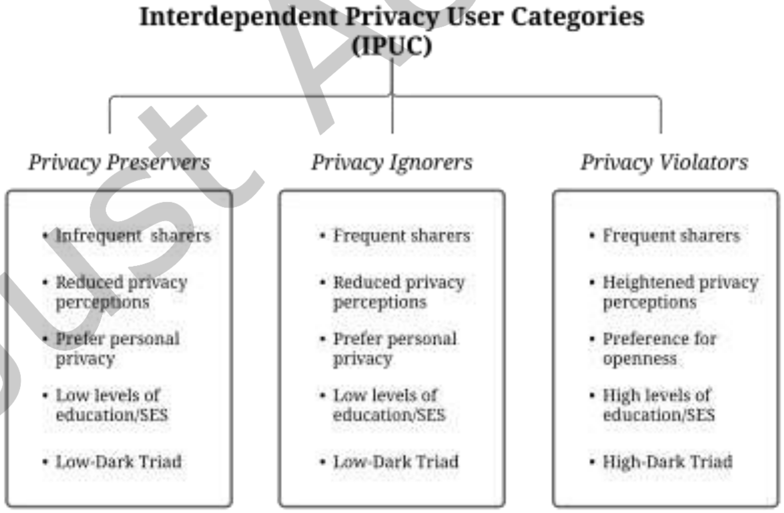
Interdependent Privacy User Categories
(IPUC)
Privacy Preservers
• Infrequent sharers
• Reduced privacy perceptions
• Prefer personal privacy
• Low levels of education/SES
• Low-Dark Triad
Privacy Ignorers
• Frequent sharers
• Reduced privacy perceptions
• Prefer personal privacy
• Low levels of education/SES
• Low-Dark Triad
Privacy Violators
• Frequent sharers
• Heightened privacy perceptions
• Preference for openness
• High levels of education/SES
• High-Dark Triad

Figure 4: Key characteristics of interdependent privacy user categories detected using cluster analysis.

5.6 Demographic differences in interdependent privacy perceptions

In addition to uncovering several significant linkages between user personality and interdependent privacy perceptions, we examined individual differences pertaining to demographic background. When examining participant demographics, we found that higher levels of education and SES were associated with increased privacy ratings. However, despite widely reported generational differences in social media behaviors [9,50,77], user age was not significantly related to interdependent privacy perceptions. Examining the effect as one of marginal statistical significance (p = .09)[1], higher age was associated with lower privacy ratings.

Taken together, associations between education, SES, and interdependent privacy beliefs may be understood in the context of digital literacy [24]. Although the exact definition of digital literacy varies, it generally describes the knowledge and skills needed for effective online communication [64]. Previous research reports the existence of a 'digital divide' with significant demographic disparities in digital literacy and online skills [20,21,24,37,91], which are necessary for effective maintenance of personal privacy [24,36,82]. Our findings indicate that disparities in personal privacy and digital literacy may extend to interdependent privacy behaviors as well, where people with greater educational access and presumably exposure to social media at earlier ages indicate higher awareness of interdependent privacy. Furthermore, our results align with earlier research on interdependent privacy reporting that user demographics were strong predictors of privacy preferences [15].

5.7 Interdependent privacy as a function of social media usage

Finally, we examined social media usage and photo sharing behaviors, showing that social media usage is a key predictor of privacy perceptions. For example, we found that users who frequently visit social media perceive memes as less private, while users who share a greater number of photos perceive them as more private. We suspect that user perceptions of privacy correspond to the user's level of experience with different types of online activities. That is, users who more frequently visit social media may have diminished privacy perceptions because of their continual exposure to photos and information about others. Comparatively, users that share more photos themselves gain experience evaluating the appropriateness of the images they share, perhaps leading to an increased awareness of interdependent privacy issues. This conclusion is supported by a recent five-year analysis of privacy perceptions on Facebook which concluded that users who were more active on Facebook perceived the internet as less of a privacy threat [108]. In addition to contributing to privacy perceptions, there is also evidence that user preferences regarding privacy interventions is associated with sharing frequency, with more frequent sharers preferring methods that do not interfere with ease of sharing [15]. While there are some studies examining the relationship between social media usage and privacy preferences [47], more research is needed to determine how privacy attitudes evolve over time corresponding to user experience.

[1] We opt to acknowledge marginal effects in our results. This is consistent with arguments that p-values and effect sizes should be interpreted as a continuous variable, where interpretations of confidence in rejecting the null hypothesis should lie along a continuum [4].

5.8 Design implications

The current research identifies user characteristics relevant to interdependent privacy evaluations, with the aim of informing interventions that are sensitive to individual differences in privacy perceptions. Identifying user types with distinct privacy perceptions and social media behaviors is an important first step in developing targeted intervention strategies. Next, we discuss how these findings can be used to inform the design of interdependent privacy interventions.

Our findings suggest that certain user types might benefit from privacy literacy, or education about interdependent privacy on social media more than others. This is supported by several observations: The average privacy perception of participants in the current study was relatively low considering that our stimuli contained several images of social security cards, sexual information, and photos depicting children negatively (i.e., a vulnerable population). Next, our cluster analysis identified a group of users (i.e., "privacy ignorers") who frequently share images of strangers but do not appear to evaluate photo-based memes of strangers in compromising situations as too private to share. Third, we observed demographic differences in interdependent privacy perceptions that were consistent with a 'digital divide' in privacy literacy [91]. Thus, interventions that focus on educating users about interdependent privacy and photo sharing are likely important for supporting interdependent privacy preservation on social media. These approaches may also help reduce disparities in privacy literacy by increasing access to educational resources for users who are less familiar with various privacy issues.

In addition, identifying user characteristics that influence sharing behaviors can help with the design of targeted nudge-based interventions. Privacy nudges, or reminders aimed at discouraging privacy violations [49], are put forth as a method of limiting self-disclosures on social media, but evidence supporting their effectiveness for interdependent privacy issues has been mixed [3,7,49,110,123]. One explanation as to why some researchers have failed to influence sharing behaviors via nudging is that their effectiveness depends on user characteristics and framing [49]. Earlier work reports large increases in nudging effectiveness when messages were tailored to fit user demographics [59] and decision making styles [85]. As such, we identified a group of users with notably elevated sensitivity towards potential privacy issues and frequent disclosures on social media. Nudges may not be as effective if providing redundant information or targeting strong personal preferences [110,119]. Thus, we suspect these users could be less receptive to nudging depending on their familiarity or experience level. An alternative for dissuading users with high privacy literacy could involve the use of concrete incentives and disincentives, such as the warning system proposed by Cherubini et al. [15] which notifies the users of the consequences for sharing inappropriate private content during the upload process.

Finally, while numerous other methods for limiting interdependent privacy have been proposed in the MPP literature, such as negotiation tools [13,102,103], voting mechanisms [44], and automatic notification systems [121], these collaborative approaches are not as applicable to viral memes. Technical approaches that automatically hide private information in photos by blurring or obfuscation [48] may be a more appropriate solution to privacy concerns related to widely re-shared content. Consistent with previous reports [117], our findings suggest perceived privacy risks can be a barrier to sharing on social media, particularly when the content has limited entertainment value. Thus, research on obfuscation attempting to limit the impact of image alteration on user satisfaction, e.g., [39,41,67], is well positioned to minimize privacy concerns while maximizing social connectedness.

6 LIMITATIONS AND FUTURE DIRECTIONS

Although we used real-world memes collected from social media, a limitation of the study was that we relied on self-report data to assess how often users shared memes and other types of photos on their own social media accounts. It is possible that participants mischaracterized or misremembered their own social media behaviors; thus, an important next step is to analyze how real social media activity corresponds to self-reported personality and user traits. Further, it would be helpful to compare self-reported privacy perceptions to real-world sharing behaviors related to privacy preservation. Relatedly, we are specific in analyzing privacy perceptions of memes, however, users participate in many types of interdependent privacy violations. For example, users often re-share private posts of other users in more public context, i.e., re-posting someone's private Facebook post to a public page on Reddit. Memes can also be formatted in a variety of ways themselves, including as photos with captions, drawings, or videos. The memes we analyzed represented a specific class of privacy violation involving the re-sharing of a stranger's personal information for entertainment purposes, but more research is needed to understand how our findings on interdependent privacy perceptions translate to different content.

In addition, because we do not collect data from social media, we do not consider how user sharing behavior varies by social media platform. Certain platforms, like Reddit or Twitter, are more anonymous than those requiring stricter verification, and the behavior of anonymous users likely differs from that displayed by Facebook users who are connected to friends and family. It is also possible that the threshold for what is considered 'too private to share' differs by website depending on community preferences or website guidelines. Follow-up studies may want to consider how the privacy attitudes reported are platform specific. Similarly, our research was restricted to active social media users, but future research may expand to consider how privacy and sharing preferences vary between active social media users and those who opt out of online posting. Our research is also limited in relying on responses collected from Amazon Mechanical Turk, where these respondents may differ from the general population. However, research by Redmiles and colleagues [89] supports the notion security and privacy research carried out on Amazon Mechanical Turk yields sufficient generalizability.

Finally, we should note clustering was used to identify the distinct user privacy types presented in the IPUC model as we believed this approach would be more objective than qualitative descriptions alone. Cluster analysis with k-prototyping is a relatively simple approach that is susceptible to biases in the data, and it may be difficult to replicate the exact clusters we found in different samples or populations. Despite, these inherent limitations, the results of our analysis are consistent with the literature on dark triad personality types, Westin's conceptualizations [115], and our other statistical results. Thus, we believe the IPUC model provides a helpful framework for future researchers investigating the relationship between user characteristics and privacy preferences, particularly when investigating personality or privacy literacy.

7 CONCLUSIONS

This project expands on previous interdependent privacy literature in the following ways: First, we focus on privacy perceptions and sharing standards for real-world photo-based memes—that included potentially compromising photos of people—to understand user characteristics (esp. personality) associated with the spread of other people's information on social media. In particular, users high in dark triad characteristics rated photo-based memes as more private and were also more likely to share information about other people. Second, we identify key motivating factors for sharing potentially sensitive photos of strangers on social media. The likelihood of sharing an image-based meme was influenced by the degree to which that meme was perceived as private; however, this relationship depended on the entertainment value of the image. Third, in addition to establishing "normative" or average user characteristics, we are the first to identify distinct user types that vary in their interdependent privacy perceptions and behaviors, including privacy preservers, ignorers, and violators. Lastly, we uncover findings with significant implications for interventions aimed to decrease interdependent privacy violations on social media. Our results that identify distinct user types that vary in interdependent privacy preferences suggest the need for targeted intervention strategies, versus a one-size-fits-all approach.

REFERENCES

[1] Paul Allison. 1999. *Multiple regression: A primer.* Pine Forge Press, Thousand Oaks, CA.

[2] Mary J. Amon. 2017. Looking through the glass ceiling: A qualitative study of STEM women's career narratives. *Frontiers in Psychology* 8, 236 (2017). DOI:https://doi.org/10.3389/fpsyg.2017.00236

[3] Mary J. Amon, Rakibul Hasan, Kurt Hugenberg, Bennett I. Bertenthal, and Apu Kapadia. 2020. Influencing photo sharing decisions on social media: A case of paradoxical findings. In *2020 IEEE Symposium on Security and Privacy*, IEEE, 1350–1366. DOI:https://doi.org/doi:10.1109/SP.2020.00006

[4] Chittaranjan Andrade. 2019. The p value and statistical significance: misunderstandings, explanations, challenges, and alternatives. *Indian Journal of Psychological Medicine* 41, 3 (2019), 210–215. DOI:https://doi.org/10.4103/IJPSYM.IJPSYM_193_19

[5] Vimala Balakrishnan, Shahzaib Khan, Terence Fernandez, and Hamid R. Arabnia. 2019. Cyberbullying detection on twitter using Big Five and Dark Triad features. *Personality and individual differences* 141, (2019), 252–257. DOI:https://doi.org/10.1016/j.paid.2019.01.024

[6] Susan B. Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11, 9 (2006), 1–13. DOI:https://doi.org/doi:10.5210/fm.v11i9.1394

[7] Omri Ben-Shahar and Adam Chilton. 2016. Simplification of Privacy Disclosures: An Experimental Test. *The Journal of Legal Studies* 45, S2 (June 2016), S41–S67. DOI:https://doi.org/10.1086/688405

[8] Andrew Besmer and Heather Lipford. 2010. Moving beyond untagging: Photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1563–1572. DOI:https://doi.org/10.1145/1753326.1753560

[9] Victoria Bordonaba-Juste, Laura Lucia-Palacios, and Raúl Pérez-López. 2020. Generational differences in valuing usefulness, privacy and security negative experiences for paying for cloud services. *Information Systems and e-Business Management* 18, 1 (2020), 35–60. DOI:https://doi.org/10.1007/s10257-020-00462-8

[10] Danah M. Boyd. 2008. Taken out of context: American teen sociality in networked publics. University of California, Berkeley, ProQuest Dissertations Publishing.

[11] Danah M. Boyd. 2014. *It's complicated: The social lives of networked teens.* Yale University Press.

[12] Laura Bufardi and Keith Campbell. 2008. Narcissism and social networking ties on the internet'. *Personality and Social Psychology Bulletin* 34, 10 (2008), 1303–14.

[13] Barbara Carminati and Elena Ferrari. 2012. Collaborative access control in online social networks. In *7th International Conference on Collaborative Computing: Networking, Applications and Worksharing.*

[14] Jin Chen, Jerry W. Ping, Yunjie Xu, and Bernard C. Y. Tan. 2015. Information privacy concern about peer disclosure in online social networks. *IEEE Transactions on Engineering Management* 62, 3 (2015), 311–324. DOI:https://doi.org/10.1109/TEM.2015.2432117

[15] Mauro Cherubini, Kavous Salehzadeh Niksirat, Marc-Olivier Boldi, Henri Keopraseuth, Jose M. Such, and Kévin Huguenin. 2021. When forcing collaboration is the most sensible choice: Desirability of precautionary and dissuasive mechanisms to manage multiparty privacy conflicts. In *Proceedings of the ACM on Human-Computer Interaction*, 1–36. DOI:https://doi.org/10.1145/3449127

[16] Kai L. Chung, Izzat Morshidi, Lee C. Yoong, and Kher N. Thian. 2019. The role of the dark tetrad and impulsivity in social media addiction: Findings from Malaysia. *Personality and Individual Differences* 143, (2019), 62–67. DOI:https://doi.org/10.1016/j.paid.2019.02.016

[17] Lucie Corcoran, Irene Connolly, and Mona O'Moore. 2012. Cyberbullying in Irish schools: An investigation of personality and self-concept. *The Irish Journal of Psychology* 33, 4 (2012), 153–165. DOI:https://doi.org/10.1080/03033910.2012.677995

[18] Laura C. Crysel, Benjamin S. Crosier, and Gregory D. Webster. 2013. The Dark Triad and risk behavior. *Personality and Individual Differences* 54, 1 (2013), 35–40. DOI:https://doi.org/10.1016/j.paid.2012.07.029

[19] Zeynep I. Demircioğlu and Aslı G. Köse. 2021. Effects of attachment styles, dark triad, rejection sensitivity, and relationship satisfaction on social media addiction: A mediated model. *Current Psychology* 40, (2021), 414–428. DOI:https://doi.org/10.1007/s12144-018-9956-x

[20] Alexander van Deursen and Jan van Dijk. 2015. Internet skill levels increase, but gaps widen: a longitudinal cross-sectional analysis (2010–2013) among the Dutch population. *Information, Communication & Society* 18, 7 (2015), 782–797. DOI:https://doi.org/10.1080/1369118X.2014.994544

[21] Jan van Dijk. 2020. *The digital divide*. John Wiley & Sons. Retrieved January 23, 2022 from https://www.wiley.com/en-us/The+Digital+Divide-p-9781509534456

[22] Michael Dufner, Jochen E. Gebauer, Constantine Sedikides, and Jaap J. A. Denissen. 2019. Self-enhancement and psychological adjustment: A meta-analytic review. *Personality and Social Psychology Review* 23, 1 (2019), 48–72. DOI:https://doi.org/10.1177/1088868318756467

[23] Regina J.J.M. van den Eijnden, Jeroen S. Lemmens, and Patti M. Valkenburg. 2016. The social media disorder scale. *Computers in Human Behavior* 61, (2016), 478–487. DOI:https://doi.org/10.1016/j.chb.2016.03.038

[24] Dmitry Epstein and Kelly Quinn. 2020. Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society* 6, 2 (2020). DOI:https://doi.org/10.1177/2056305120916853

[25] Anthony M. Evans and William Revelle. 2008. Survey and behavioral measurements of interpersonal trust. *Journal of Research in Personality* 42, 6 (2008), 1585–1593. DOI:https://doi.org/10.1016/j.jrp.2008.07.011

[26] Lisa Fazio. 2020. Out-of-context photos are a powerful low-tech form of misinformation. *The Conversation*. Retrieved from https://theconversation.com/out-of-context-photos-are-a-powerful-low-tech-form-of-misinformation-129959/

[27] Christopher J. Ferguson. 2009. An effect size primer: A guide for clinicians and researchers. *Professional Psychology: Research and Practice* 40, 5 (October 2009), 532–538. DOI:https://doi.org/10.1037/a0015808

[28] Ruth Festl and Thorsten Quandt. 2013. Social relations and cyberbullying: The influence of individual and structural attributes on victimization and perpetration via the internet. *Human Communication Research* 39, 1 (2013), 101–126. DOI:https://doi.org/10.1111/j.1468-2958.2012.01442.x

[29] Jesse Fox and Margaret C. Rooney. 2015. The Dark Triad and trait self-objectification as predictors of men's use and self-presentation behaviors on social networking sites. *Personality and Individual Differences* 76, (2015), 161–165. DOI:https://doi.org/10.1016/j.paid.2014.12.017

[30] Siyao Fu, Haibo He, and Zeng-Guang Hou. 2014. Learning Race from Face: A Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 36, 12 (December 2014), 2483–2509. DOI:https://doi.org/10.1109/TPAMI.2014.2321570

[31] Mitch van Geel, Anouk Goemans, Fatih Toprak, and Paul Vedder. 2017. Which personality traits are related to traditional bullying and cyberbullying? A study with the Big Five, Dark Triad and sadism. *Personality and Individual Differences* 106, (2017), 231–235. DOI:https://doi.org/10.1016/j.paid.2016.10.063

[32] Zebbedia G. Gibb and Paul G. Devereux. 2014. Who does that anyway? Predictors and personality correlates of cyberbullying in college. *Computers in Human Behavior* 38, (2014), 8–16. DOI:https://doi.org/10.1016/j.chb.2014.05.009

[33] Lewis R. Goldberg. 1990. An alternative "description of personality": The Big-Five factor structure. *Journal of Personality and Social Psychology* 59, 6 (1990), 1216–1229. DOI:https://doi.org/10.1037/0022-3514.59.6.1216

[34] Alan K. Goodboy and Matthew M. Martin. 2015. The personality profile of a cyberbully: Examining the Dark Triad. *Computers in Human Behavior* 49, (2015), 1–4. DOI:https://doi.org/10.1016/j.chb.2015.02.052

[35] Samuel D. Gosling, Peter J. Rentfrow, and William B. Swann. 2003. A very brief measure of the Big-Five personality domains. *Journal of Research in Personality* 37, 6 (2003), 504–528. DOI:https://doi.org/10.1016/S0092-6566(03)00046-1

[36] Loni Hagen. 2017. Overcoming the privacy challenges of wearable devices: A study on the role of digital literacy. In *Proceedings of the 18th Annual International Conference on Digital Government Research* (dg.o '17), Association for Computing Machinery, New York, NY, USA, 598–599. DOI:https://doi.org/10.1145/3085228.3085254

[37] Eszter Hargittai. 2010. Digital na (t) ives? Variation in internet skills and uses among members of the "net generation." *Sociological Inquiry* 80, 1 (2010), 92–113. DOI:https://doi.org/10.1111/j.1475-682X.2009.00317.x

[38] Spencer E. Harpe. 2015. How to analyze Likert and other rating scale data. *Currents in Pharmacy Teaching and Learning* 7, 6 (November 2015), 836–850. DOI:https://doi.org/10.1016/j.cptl.2015.08.001

[39] Eman Hasan, Rakibul Hasan, Patrick Shaffer, David Crandall, and Apu Kapadia. 2017. Cartooning for enhanced privacy in lifelogging and streaming videos. 29–38.

[40] Rakibul Hasan, Bennett I. Bertenthal, Kurt Hugenberg, and Apu Kapadia. 2021. Your photo is so funny that I don't mind violating your privacy by sharing it: Effects of individual humor styles on online photo-sharing behaviors. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (CHI '21), Association for Computing Machinery, New York, NY, USA. DOI:https://doi.org/10.1145/3411764.3445258

[41] Rakibul Hasan, Yifang Li, Eman Hassan, Kelly Caine, David J. Crandall, Roberto Hoyle, and Apu Kapadia. 2019. Can Privacy Be Satisfying? On Improving Viewer Satisfaction for Privacy-Enhanced Photos Using Aesthetic Transforms. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19), Association for Computing Machinery, New York, NY, USA, 1–13. DOI:https://doi.org/10.1145/3290605.3300597

[42] Benjamin Henne, Christian Szongott, and Matthew Smith. 2013. SnapMe if you can: Privacy threats of other peoples' geo-tagged media and what we can do about it. In *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks* (WiSec '13), Association for Computing Machinery, New York, NY, USA, 95–106. DOI:https://doi.org/10.1145/2462096.2462113

[43] Roberto Hoyle, Luke Stark, Qatrunnada Ismail, David Crandall, Apu Kapadia, and Denise Anthony. 2020. Privacy norms and preferences for photos posted online. *ACM Transactions on Computer-Human Interaction* 27, 4 (2020), 1–27. DOI:https://doi.org/10.1145/3380960

[44] Qinlong Huang, Yixian Yang, Wei Yue, and Yue He. 2021. Secure data group sharing and conditional dissemination with multi-owner in cloud computing. *IEEE Transactions on Cloud Computing* 9, 4 (October 2021), 1607–1618. DOI:https://doi.org/10.1109/TCC.2019.2908163

[45] Zhexue Huang. 1998. Extensions to the k-means algorithm for clustering large data sets with categorical values. *Data Mining and Knowledge Discovery* 2, 3 (1998), 283–304. DOI:https://doi.org/10.1023/A:1009769707641

[46] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A survey on interdependent privacy. *ACM Computing Surveys* 52, 6 (2019), 1–40. DOI:https://doi.org/10.1145/3360498

[47] Gary L. Hunter and Steven A. Taylor. 2020. The relationship between preference for privacy and social media usage. *Journal of Consumer Marketing* 37, 1 (2020), 43–54. DOI:https://doi.org/10.1108/JCM-11-2018-2927

[48] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/off: Preventing privacy leakage from photos in social networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (CCS '15), Association for Computing Machinery, New York, NY, USA, 781–792. DOI:https://doi.org/10.1145/2810103.2813603

[49] Athina Ioannou, Lis Tussyadiah, Graham Miller, Shujun Li, and Mario Weick. 2021. Privacy nudges for disclosure of personal information: A systematic literature review and meta-analysis. *PLOS ONE* 16, 8 (2021). DOI:https://doi.org/10.1371/journal.pone.0256822

[50] Mengtian Jiang, Hsin-yi Sandy Tsai, Shelia R. Cotten, Nora J. Rifon, Robert LaRose, and Saleem Alhabash. 2016. Generational differences in online safety perceptions, knowledge, and practices. *null* 42, 9 (September 2016), 621–634. DOI:https://doi.org/10.1080/03601277.2016.1205408

[51] Daniel N. Jones and Delroy L. Paulhus. 2010. Differentiating the Dark Triad within the interpersonal circumplex. In *Handbook of interpersonal psychology: Theory, research, assessment and therapeutic interventions*. John Wiley & Sons, Inc., 249–267.

[52] Daniel N. Jones and Delroy L. Paulhus. 2011. The role of impulsivity in the Dark Triad of personality. *Personality and Individual Differences* 51, 5 (2011), 679–682. DOI:https://doi.org/10.1016/j.paid.2011.04.011

[53] Daniel N. Jones and Delroy L. Paulhus. 2014. Introducing the short dark triad (SD3): A brief measure of dark personality traits. *Assessment* 21, 1 (2014), 28–41. DOI:https://doi.org/10.1177/1073191113514105

[54] Iris A. Junglas, Norman A. Johnson, and Christiane Spitzmüller. 2008. Personality traits and concern for privacy: An empirical study in the context of location-based services. *null* 17, 4 (2008), 387–402. DOI:https://doi.org/10.1057/ejis.2008.29

[55] Sanjay Kairam, Joseph Kaye, John A. Guerra-Gomez, and David A. Shamma. 2016. Snap decisions? How users, content, and aesthetics interact to shape photo sharing behaviors. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), Association for Computing Machinery, New York, NY, USA, 113–124. DOI:https://doi.org/10.1145/2858036.2858451

[56] Leonard Kaufman and Peter J. Rousseeuw. 2009. *Finding groups in data: An introduction to cluster analysis.* John Wiley & Sons, Hoboken, NY, USA.

[57] Scott Barry Kaufman, David Bryce Yaden, Elizabeth Hyde, and Eli Tsukayama. 2019. The light vs. dark triad of personality: Contrasting two very different profiles of human nature. *Frontiers in Psychology* 10, (2019), 1–26. DOI:https://doi.org/10.3389/fpsyg.2019.00467

[58] Kagan Kircaburun, Zsolt Demetrovics, and Şule B. Tosuntaş. 2019. Analyzing the links between problematic social media use, Dark Triad traits, and self-esteem. *International Journal of Mental Health and Addiction* 17, 6 (2019), 1496–1507. DOI:https://doi.org/10.1007/s11469-018-9900-1

[59] Bart P. Knijnenburg and Alfred Kobsa. 2013. Helping users with information disclosure decisions: potential for adaptation. In *Proceedings of the 2013 international conference on Intelligent user interfaces* (IUI '13), Association for Computing Machinery, New York, NY, USA, 407–416. DOI:https://doi.org/10.1145/2449396.2449448

[60] Nadin Kökciyan, Nefise Yaglikci, and Pinar Yolum. 2017. An Argumentation Approach for Resolving Privacy Disputes in Online Social Networks. *ACM Trans. Internet Technol.* 17, 3 (August 2017), 1–22. DOI:https://doi.org/10.1145/3003434

[61] Robin M. Kowalski. 2001. *Behaving badly: Aversive behaviors in interpersonal relationships.* American Psychological Association, Washington, DC, US. DOI:https://doi.org/10.1037/10365-000

[62] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: Interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), Association for Computing Machinery, New York, NY, USA, 3217–3226. DOI:https://doi.org/10.1145/1978942.1979420

[63] Colin Lankshear and Michele Knobel. 2007. A new literacies sampler. In *A pedagogy of multiliteracies: Designing social futures. Harvard Educational Review.* New York: Peter Lang. New London Group., 60–92.

[64] Nancy Law, David Woo, Jimmy Torre, and Gary Wong. 2018. *A global framework of reference on digital literacy skills for indicator 4.4.2.* UNESCO Institute for Statistics, Montreal. Retrieved from http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf

[65] Namyeon Lee and Ohbyung Kwon. 2015. A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. *Expert Systems with Applications* 42, 5 (April 2015), 2764–2771. DOI:https://doi.org/10.1016/j.eswa.2014.11.031

[66] Yifang Li, Nishant Vishwamitra, Hongxin Hu, and Kelly Caine. 2020. Towards a taxonomy of content sensitivity and sharing preferences for photos. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Association for Computing Machinery, New York, NY, USA, 1–14. Retrieved from https://doi.org/10.1145/3313831.3376498

[67] Yifang Li, Nishant Vishwamitra, Bart P. Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW (December 2017), 67:1-67:24. DOI:https://doi.org/10.1145/3134702

[68] Barbara Lopes and Hui Yu. 2017. Who do you troll and why: An investigation into the relationship between the Dark Triad Personalities and online trolling behaviours towards popular and less popular Facebook profiles. *Computers in Human Behavior* 77, (2017), 69–76. DOI:https://doi.org/10.1016/j.chb.2017.08.036

[69] Petar Lukić and Marko Živanović. 2021. Shedding light on the Light Triad: Further evidence on structural, construct, and predictive validity of the Light Triad. *Personality and Individual Differences* 178, (2021), 110876. DOI:https://doi.org/10.1016/j.paid.2021.110876

[70] Marta Malesza and Paweł Ostaszewski. 2016. Dark side of impulsivity—Associations between the Dark Triad, self-report and behavioral measures of impulsivity. *Personality and Individual Differences* 88, (2016), 197–201. DOI:https://doi.org/10.1016/j.paid.2015.09.016

[71] Huina Mao, Xin Shuai, and Apu Kapadia. 2011. Loose tweets: an analysis of privacy leaks on twitter. In *Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society* (WPES '11), Association for Computing Machinery, New York, NY, USA, 1–12. DOI:https://doi.org/10.1145/2046556.2046558

[72] Evita March and Jessica Z. Marrington. 2021. Antisocial and prosocial online behaviour: Exploring the roles of the Dark and Light Triads. *Current Psychology* (2021). DOI:https://doi.org/10.1007/s12144-021-01552-7

[73] Ahmed A. Marouf, Rasif Ajwad, and Adnan F. Ashrafi. 2019. Looking behind the mask: A framework for detecting character assassination via troll comments on social media using psycholinguistic tools. In *2019 International Conference on Electrical, Computer and Communication Engineering*. DOI:https://doi.org/10.1109/ECACE.2019.8679154

[74] Jessica L. McCain, Zachary G. Borg, Ariel H. Rothenberg, Kristina M. Churillo, Paul Weiler, and Keith Campbell. 2016. Personality and selfies: Narcissism and the Dark Triad. *Computers in Human Behavior* 64, (2016), 126–133. DOI:https://doi.org/10.1016/j.chb.2016.06.050

[75] Nora McDonald and Andrea Forte. 2020. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Association for Computing Machinery, New York, NY, USA, 1–14. DOI:https://doi.org/10.1145/3313831.3376167

[76] Soraya Mehdizadeh. 2010. Self-presentation 2.0: Narcissism and self-esteem on Facebook. *Cyberpsychology, Behavior, and Social Networking* 13, 4 (2010), 357–364. DOI:https://doi.org/10.1089/cyber.2009.0257

[77] Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. 2014. Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems* 23, 2 (2014), 103–125. DOI:https://doi.org/10.1057/ejis.2013.17

[78] Graeme R. Newman and Megan N. McNally. 2005. Identity theft literature review. *National Institute of Justice*. Retrieved January 23, 2022 from https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-theft-literature-review

[79] David H. Nguyen, Gabriela Marcu, Gillian R. Hayes, Khai N. Truong, James Scott, Marc Langheinrich, and Christof Roduner. 2009. Encountering SenseCam: personal recording technologies in everyday life. In *Proceedings of the 11th International Conference on Ubiquitous Computing* (UbiComp '09), Association for Computing Machinery, New York, NY, USA, 165–174. DOI:https://doi.org/10.1145/1620545.1620571

[80] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press. DOI:https://doi.org/doi:10.1515/9780804772891

[81] Babajide Osatuyi. 2015. Personality traits and information privacy concern on social media platforms. *Journal of Computer Information Systems* 55, 4 (2015), 11–19. DOI:https://doi.org/10.1080/08874417.2015.11645782

[82] Yong J. Park. 2013. Digital literacy and privacy behavior online. *Communication Research* 40, 2 (April 2013), 215–236. DOI:https://doi.org/10.1177/0093650211418338

[83] Justin W. Patchin and Sameer Hinduja. 2020. Sextortion among adolescents: Results from a national survey of US youth. *Sex Abuse* 32, 1 (2020), 30–54. DOI:https://doi.org/10.1177/1079063218800469

[84] Delroy L. Paulhus and Kevin M. Williams. 2002. The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality* 36, 6 (December 2002), 556–563. DOI:https://doi.org/10.1016/S0092-6566(02)00505-6

[85] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. 2020. Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavior* 109, (August 2020), 106347. DOI:https://doi.org/10.1016/j.chb.2020.106347

[86] Beatrice Rammstedt and Oliver P. John. 2007. Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German. *Journal of Research in Personality* 41, 1 (2007), 203–212. DOI:https://doi.org/10.1016/j.jrp.2006.02.001

[87] Yasmeen Rashidi, Tousif Ahmed, Felicia Patel, Emily Fath, Apu Kapadia, Christena Nippert-Eng, and Norman M. Su. 2018. "You don't want to be the next meme": College students' workarounds to manage privacy in the era of pervasive photography. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, USENIX Association, Baltimore, MD, 143–157. Retrieved from https://www.usenix.org/conference/soups2018/presentation/rashidi

[88] Yasmeen Rashidi, Apu Kapadia, Christena Nippert-Eng, and Norman M. Su. 2020. "It's easier than causing confrontation": Sanctioning strategies to maintain social norms and privacy on social media. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW1 (2020), 1–25. DOI:https://doi.org/10.1145/3392827

[89] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*, 1326–1343. DOI:https://doi.org/10.1109/SP.2019.00014

[90] Sarah T. Roberts. 2019. *Behind the screen: Content moderation in the shadows of social media.* Yale University Press. DOI:https://doi.org/doi:10.12987/9780300245318

[91] Laura Robinson, Shelia R. Cotten, Hiroshi Ono, Anabel Quan-Haase, Gustavo Mesch, Wenhong Chen, Jeremy Schulz, Timothy M. Hale, and Michael J. Stern. 2015. Digital inequalities and why they matter. *Information, Communication & Society* 18, 5 (May 2015), 569–582. DOI:https://doi.org/10.1080/1369118X.2015.1012532

[92] Jenny Rosenberg and Nichole Egbert. 2011. Online impression management: Personality traits and concerns for secondary goals as predictors of self-presentation tactics on Facebook. *Journal of Computer-Mediated Communication* 17, 1 (2011), 1–18. DOI:https://doi.org/10.1111/j.1083-6101.2011.01560.x

[93] Minna Ruckenstein and Linda Turunen. 2020. Re-humanizing the platform: Content moderators and the logic of care. *New Media & Society* 22, 6 (June 2020), 1026–1042. DOI:https://doi.org/10.1177/1461444819875990

[94] Triantoro Safaria, Fathul Lubabin, Eny Purwandari, Eka Zenita Ratnaningsih, Maya Khairani, Nofrans Eka Saputra, Erna Ipak Rahmawati, Zulaeni Esita, Dina Nazriani, and Miftahuddin Miftahuddin. 2020. The role of dark triad personality on cyberbullying: Is it still a problem? *International Journal of Scientific & Technology Research* 9, 2 (2020), 4256–4260.

[95] Elżbieta Sanecka. 2017. The dark side of social media: Associations between the Dark Triad of personality, self-disclosure online and selfie-related behaviours. *The Journal of Education, Culture, and Society* 8, 2 (2017), 71–88.

[96] Mustafa Savci. 2019. Social media craving and the amount of self-disclosure: The mediating role of the Dark Triad. *International Online Journal of Educational Sciences* 11, 4 (2019).

[97] Barış Sevi and Burak Doğruyol. 2020. Looking from the bright side: The Light Triad predicts Tinder use for love. *Journal of Social and Personal Relationships* 37, 7 (2020), 2136–2144. DOI:https://doi.org/10.1177/0265407520918942

[98] Limor Shifman. 2013. Memes in a digital world: Reconciling with a conceptual troublemaker. *Journal of Computer-Mediated Communication* 18, 3 (2013), 362–377. DOI:https://doi.org/10.1111/jcc4.12013

[99] Jae Woong Shim, Seungwhan Lee, and Bryant Paul. 2007. Who responds to unsolicited sexually explicit materials on the internet?: The role of individual differences. *CyberPsychology & Behavior* 10, 1 (2007), 71–79. DOI:https://doi.org/10.1089/cpb.2006.9990

[100] Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. 2015. Portrait of a privacy invasion: Detecting relationships through large-scale photo analysis. *Proceedings on Privacy Enhancing Technologies* 2015, 1 (April 2015), 41–60. DOI:https://doi.org/10.1515/popets-2015-0004

[101] Shen Hin Soo, Madeline Tanamal K.Y. Tan, Ju Y. Ho, Wen L. Low, Maryam M. Yahya, and Jessica S.Y. Ho. 2015. Consumer personality, privacy concerns and usage of location-based services (LBS). *Journal of Economics, Business and Management* 3, 10 (2015).

[102] Anna C. Squicciarini, Heng Xu, and Xiaolong (Luke) Zhang. 2011. CoPE: Enabling collaborative privacy management in online social networks. *J. Am. Soc. Inf. Sci. Technol.* 62, 3 (March 2011), 521–534. DOI:https://doi.org/10.1002/asi.21473

[103] Jose M. Such and Natalia Criado. 2016. Resolving Multi-party Privacy Conflicts in Social Media. *IEEE Trans. Knowl. Data Eng.* 28, 7 (July 2016), 1851–1863. DOI:https://doi.org/10.1109/TKDE.2016.2539165

[104] Jose M. Such and Natalia Criado. 2018. Multiparty privacy in social media. *Commun. ACM* 61, 8 (July 2018), 74–81. DOI:https://doi.org/10.1145/3208039

[105] Jose M. Such, Joel Porter, Sören Preibusch, and Adam Joinson. 2017. Photo Privacy Conflicts in Social Media: A Large-scale Empirical Study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, Denver Colorado USA, 3821–3832. DOI:https://doi.org/10.1145/3025453.3025668

[106] Gero Szepannek. 2018. clustMixType: User-friendly clustering of mixed-type data in R. *R Journal* 10, 2 (2018), 200–209.

[107] Kurt Thomas, Chris Grier, and David M. Nicol. 2010. unFriendly: Multi-party privacy risks in social networks. In *Privacy Enhancing Technologies* (Lecture Notes in Computer Science), Springer, Berlin, Heidelberg, 236–252. DOI:https://doi.org/10.1007/978-3-642-14527-8_14

[108] Mina Tsay-Vogel, James Shanahan, and Nancy Signorielli. 2018. Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society* 20, 1 (January 2018), 141–161. DOI:https://doi.org/10.1177/1461444816660731

[109] Jennifer M. Urban and Chris J. Hoofnagle. 2014. The privacy pragmatic as privacy vulnerable. In *Symposium on Usable Privacy and Security (SOUPS 2014) Workshop on Privacy Personas and Segmentation (PPS).*

[110] Tina A. G. Venema, Floor M. Kroese, Emely De Vet, and Denise T. D. De Ridder. 2019. The One that I Want: Strong personal preferences render the center-stage nudge redundant. *Food Quality and Preference* 78, (December 2019), 103744. DOI:https://doi.org/10.1016/j.foodqual.2019.103744

[111] Fernanda B. Viégas. 2005. Bloggers' expectations of privacy and accountability: An initial survey. *Journal of Computer-Mediated Communication* 10, 3 (2005). DOI:https://doi.org/10.1111/j.1083-6101.2005.tb00260.x

[112] Michael Wai and Niko Tiliopoulos. 2012. The affective and cognitive empathic nature of the dark triad of personality. *Personality and Individual Differences* 52, 7 (2012), 794–799. DOI:https://doi.org/10.1016/j.paid.2012.01.008

[113] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro G. Leon, and Lorrie F. Cranor. 2011. "I regretted the minute I pressed share" a qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (SOUPS '11), Association for Computing Machinery, New York, NY, USA. DOI:https://doi.org/10.1145/2078827.2078841

[114] Alan F. Westin. 1967. Privacy and freedom Atheneum. *New York* 7, (1967), 431–453.

[115] Alan F. Westin. 2003. Social and political dimensions of privacy. *Journal of social issues* 59, 2 (2003), 431–453.

[116] Robert E. Wilson, Samuel D. Gosling, and Lindsay T. Graham. 2012. A review of Facebook research in the social sciences. *Perspect Psychol Sci* 7, 3 (May 2012), 203–220. DOI:https://doi.org/10.1177/1745691612442904

[117] Pamela Wisniewski, A.K.M. Najmul Islam, Bart P. Knijnenburg, and Sameer Patil. 2015. Give social network users the privacy they want. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), Association for Computing Machinery, New York, NY, USA, 1427–1441. DOI:https://doi.org/10.1145/2675133.2675256

[118] Pamela Wisniewski, AKM Islam, Heather Richter Lipford, and David C Wilson. 2016. Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. *Communications of the Association for information systems* 38, 1 (2016), 10.

[119] Pamela J. Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies* 98, (February 2017), 95–108. DOI:https://doi.org/10.1016/j.ijhcs.2016.09.006

[120] Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: coping mechanisms for sns boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Austin Texas USA, 609–618. DOI:https://doi.org/10.1145/2207676.2207761

[121] Kaihe Xu, Yuanxiong Guo, Linke Guo, Yuguang Fang, and Xiaolin Li. 2017. My Privacy My Decision: Control of Photo Sharing on Online Social Networks. *IEEE Transactions on Dependable and Secure Computing* 14, 2 (March 2017), 199–210. DOI:https://doi.org/10.1109/TDSC.2015.2443795

[122] Francisco Yus. 2021. Incongruity-resolution humorous strategies in image macro memes. *Internet Pragmatics 4*, 131–149. DOI:https://doi.org/10.1075/ip.00058.yus

[123] Bo Zhang and Heng Xu. 2016. Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16), Association for Computing Machinery, New York, NY, USA, 1676–1690. DOI:https://doi.org/10.1145/2818048.2820073