UNIVERSITY OF CALIFORNIA

Santa Barbara

The Online Privacy Divide: Understanding the Impact of Social and Digital Inequality on Privacy Concerns and Privacy Management Behaviors on Social Media

A Thesis submitted in partial satisfaction of the

requirements for the degree Master of Arts

in Communication

by

Laurent Haoyu Wang

Committee in charge:

Professor Miriam Metzger, Chair

Professor Ronald Rice

Professor Amy Gonzales

June 2023

The thesis of Laurent Haoyu Wang is approved.

_____

Amy Gonzales

_____

Ronald Rice

_____

Miriam Metzger, Committee Chair

June 2023

ACKNOWLEDGEMENTS

I am indebted to Miriam for her exceptional mentorship over the course of four years, going above and beyond her responsibilities. Thank you for introducing me to the science and the art of conducting research. During moments of academic difficulty, your unwavering support always meant a lot to me. Beyond academia, I hold Miriam in high regard as a person. Your integrity, honesty, and tenacity serve as a constant source of inspiration to me. Thank you for always pushing me to move one step further, but also telling me to slow down. Every compliment you made about me marks a milestone for me to work toward the next one. “Thank you” is never enough.

Ron is always my go-to encyclopedia. I express my gratitude to you for accepting the request of a random junior undergraduate who presented some amorphous ideas to you after class and for guiding me to transform those ideas into a concrete paper. Thank you for continuously cultivating my sense of confidence and self-efficacy during our collaborations and chats. You are always available and responsive, which clearly showcases that you are a well-established media multitasking scholar.

It was through working with Amy that motivated me to look at the world through the lens of inequality, which has largely contributed the development of my own scholarly identity and, more importantly, reminds me to be constantly appreciative of the privileges I have. I continue to happily serve as a loyal member of the Amy is Cool Society.

To my friends, my cohort, and my great colleagues—Yibei Chen, Jesse King, Jade The Salmon, Chloe Gonzales, Kylie Woodman, Ceciley Zhang, Qing Huang, Zijian Lew, Hannah Overbye, Jacova Snyder, Kyungin Kim, Xingyu Liu, Nancy Molina-Rogers, Lindsay Miller, and Paula Wang—I would never be able to thrive in my graduate school journey

without your support and inspirations on a daily basis. To all of you, I express my heartfelt gratitude for the unique experiences we have shared and the meaningful connections we have built together. Thank you for teaching me to practice self-care, to be honest with my feelings, to live my own life, and to forgive. If I were to list my favorite moments with every single one of you here, it would be a thesis in and of itself. To my "roommates," Yaxi Lyu and Linus, living with a picky and peculiar person like me has never been easy, yet you always handle it with kindness and grace. Your presence has given me permission to occasionally step away from work and has served as a legitimate excuse for me to do so.

To my parents and sister, thank you for your unconditional support throughout my six-year academic journey in the United States. You serve as remarkable role models for me to strive for excellence and as my steadfast motivation to grow stronger every day. Your constant encouragement and firm belief in me have been instrumental in shaping me into the person I am today. I dedicate this thesis to you.

ABSTRACT

The Online Privacy Divide: Understanding the Impact of Social and Digital Inequality on Privacy Concerns and Privacy Management Behaviors on Social Media

by

Laurent Haoyu Wang

Drawing from the integrated model of online privacy (Bazarova & Masur, 2020), this study examined the impacts of socioeconomic and demographic differences on privacy concerns and privacy management behaviors on social media to uncover empirical evidence for an *online privacy divide* in the U.S. In addition, this study tested generalized social trust and institutional trust as underlying mechanisms that explain divides in social media privacy concerns and behaviors. Results from an online survey (N = 1401) revealed significant differences across education (people without vs. with a college degree) and race (African Americans and Latinos vs. Whites and Asians) in privacy concerns and privacy management behaviors on both the horizontal and vertical dimensions of social media privacy. Results further supported the mediating roles that generalized social trust and institutional trust play in these relationships. Theoretical contributions to the integrated model of online privacy and to the privacy and marginalization literature are discussed. Practical implications are provided.

Keywords: privacy management, digital inequality, generalized social trust, institutional trust, the digital divide, social media

The Online Privacy Divide: Understanding the Impact of Social and Digital Inequality in Privacy Concerns and Privacy Management Behaviors on Social Media

As social media bring social, psychological, and material benefits to users (e.g., Ellison et al., 2007; Nabi et al., 2013), they continue to pose challenges to individuals' privacy. Research has extensively documented the role that psychological factors play in shaping people's privacy-related attitudes and behaviors online (e.g., Hoffmann et al., 2016; Metzger & Suh, 2017), including a privacy calculus construct, which states that people weigh the perceived benefits and costs of self-disclosure to decide the extent to which they reveal personal information online (Dienlin & Metzger, 2016; Laufer & Wolfe, 1977).

Yet a nascent research stream on privacy has started to recognize the importance of considering how individuals' socioeconomic status, historical experience, as well as learned cultural norms within certain communities, may shape privacy-related perceptions and behaviors at a group level (Epstein & Quinn, 2020; Park, 2021). Indeed, results from a handful of studies are starting to reveal preliminary evidence for a potential *online privacy divide*, suggesting that differences in one's socioeconomic and demographic backgrounds (education and race in particular) may translate into differences in privacy threats, privacy concerns (Madden, 2017), privacy management behaviors (Büchi et al., 2021), online privacy literacy (Epstein & Quinn, 2020), and privacy self-efficacy (Park, 2021).

Moreover, social media users nowadays face privacy risks posed by, and thus need to protect their privacy from, a variety of entities, including other social media users (e.g., family members, friends, and strangers) and institutions (e.g., advertisers, the government, and social media companies). One theoretical framework that speaks to these issues is the recently-proposed *integrated model of individualistic, networked, and institutional*

approaches of studying online privacy (Bazarova & Masur, 2020), which conceptualizes online privacy on horizontal (i.e., privacy vis-à-vis peers) and vertical (i.e., privacy vis-à-vis institutions) dimensions. This framework provides a means to understand conceptual nuances that may contribute to divides in social media users' privacy concerns and privacy management behaviors with regard to different audiences of personal information.

To my knowledge, Epstein and Quinn (2020) is the only study to compare socioeconomic differences in privacy management behaviors *explicitly* on the horizontal and vertical privacy dimensions, but their data primarily shed light on the impacts of age and gender. And their measures examine privacy in internet contexts that do not accommodate the unique challenges to and benefits of privacy on social media. Therefore, drawing from the integrated model of online privacy (Bazarova & Masur, 2020), the first aim of this study is to study whether there is empirical evidence for the *online privacy divide* by education and race on both the horizontal and vertical dimensions of privacy, with measures that are specifically appropriate to social media.

Further, despite preliminary evidence, critical theoretical issues remain unaddressed regarding *why* people from different sociodemographic backgrounds may form privacy concerns and engage in privacy management behaviors differently on social media. One common justification, guided by the digital divide literature, suggests that due to a lack of technological access, resources and digital skills, sociodemographically marginalized individuals may lag behind in developing online privacy awareness and privacy management skills (e.g., Büchi et al., 2021, Li et al., 2018). As a general example of how skills may impact privacy, a lack of skill at navigating mobile phone settings may limit people's ability to adjust privacy settings (e.g., turning off location tracking) on their social media accounts.

Another explanation, offered by the trust literature, may suggest that discrimination and victimization experienced by sociodemographically marginalized groups may alert them to be more careful about their online privacy, through a lack of trust, compared to non-marginalized groups (e.g., Marwick et al., 2017; Vitak et al., 2018). Indeed, compelling evidence demonstrates striking sociodemographic differences in generalized social trust and institutional trust (Madden, 2017; Taylor et al., 2007), as well as a prominent impact of trust on motivating online self-disclosure (Krasnova et al., 2010; Mesch, 2012). It is therefore possible that a lack of trust may motivate marginalized individuals to protect their privacy more vigorously on social media than non-marginalized individuals. As the role of trust in online privacy divides remains largely unknown, the second goal of this study is to test whether two types of trust–generalized social trust and institutional trust–may explain online privacy divides on the horizontal and vertical dimensions of privacy.

Results of this study stand to make several important theoretical contributions. First, this study offers the first empirical test of the integrated model of online privacy (Bazarova & Masur, 2020) with a sociodemographically diverse sample and measures tailored towards social media privacy along the horizontal and vertical privacy dimensions. Second, this study elaborates the model by theoretically advancing the mediating role of generalized social and institutional trust in social media privacy. Third, this study proposes and tests an *online privacy divide* construct, which argues that the effects of structural racism and discrimination experiences will manifest in online privacy experiences through different types of trust, beyond traditional markers of marginalization (e.g., digital access, skills). Results should not only contribute to the growing understanding of the impact of digital and social inequality in shaping people's privacy-related attitudes and behaviors on social media, but also help

extend the digital skills and digital literacy literature by drawing particular attention to online privacy management. Practically, the knowledge gained from this research can lay a foundation for better and more focused recommendations for educators, policymakers, and technology developers to help empower disadvantaged and/or marginalized social media users. Understanding privacy concerns and management practices of users from marginalized groups can help better design interventions and digital literacy training programs that are tailored to different individuals' needs.

Conceptualizing Privacy Dimensions in Social Media

Scholars have primarily conceptualized *privacy* as the ownership of or right to control personal information during interpersonal interactions (Altman, 1975; Petronio, 2002). Applying this to online contexts, people may strategically manage their privacy vis-à-vis different individuals within their online social networks. Yet in the digital media environment there are other, often invisible, audiences for our personal information, such as governments, social media companies, or marketers that collect user data for commercial purposes. As such, social media users face daunting privacy challenges because they may often want or have to simultaneously manage their privacy with regard to vastly different types of audiences and information monitoring.

The Integrated Model of Online Privacy

The recently-proposed integrated model of online privacy addresses the coexistence of different types of audiences for our personal information online (Bazarova & Masur, 2020). This model proposes the horizontal/vertical distinction of online privacy to conceptually bridge the individualistic, networked, and institutional approaches–which had been previously treated as independent levels of privacy–to studying online privacy and self-

disclosure. To elaborate, on the *horizontal* dimension, individualistic approaches highlight individuals' control of and access to personal information during online interactions; whereas networked approaches concern how technological affordances (e.g., visibility and anonymity) shape privacy boundaries between information co-owners (e.g., the individual who discloses personal information and those who then see that information online), revealing the possibility for unintended audiences to retrieve other people's private information. The horizontal dimension of privacy may encompass privacy threats posed by other social media users, within or outside of one's own social networks, and includes instances such as being terminated by an employer who sees an employee's social media posts, online stalking and harassment by others, spreading rumors, and unwanted sharing of personal information (Marwick et al., 2017; Masur & Trepte, 2021).

On the *vertical* dimension of privacy, institutional approaches involve privacy threats from social media companies, advertisers, government agencies, and other institutions that collect user data and conduct mass surveillance on users for commercial and/or administrative interests (Büchi et al., 2021). The involvement of algorithms and machine learning that automatically profile users based on their digital trace data adds additional threats to users' privacy along the vertical dimension (Madden et al., 2017). Drawing from this horizontal/vertical conceptual distinction, the following sections articulate how people from different sociodemographic backgrounds may encounter privacy risks and engage in protection behaviors on the two dimensions of privacy on social media.

The Online Privacy Divide

For people to navigate privacy threats online with regard to vastly different types of audiences and information monitoring, they must have access to resources (e.g., technology,

appropriate knowledge or training, technical support from one's own network), and develop and practice privacy management skills (Li & Chen, 2021; Li et al., 2018). However, that access can vary due to differences in education and race, among other factors.

Education and Race as Predictors

Education and race, in particular, have been demonstrated to shape gaps in accessing privacy-enhancing tools and strategies (e.g., Madden, 2017). Education is a long-standing predictor of digital skills, including privacy management. Studies have documented that less educated individuals have lower online *privacy literacy*, which includes people's understanding about the privacy practices of, and threats posed by, individuals, institutions, and online service providers (Epstein & Quinn, 2020; Madden et al., 2017). They also report lower online *privacy self-efficacy*, which is the belief in one's own ability to enact behaviors to protect online privacy (Madden et al., 2017; Park, 2021). Acquiring the practical and technical knowledge for, and gaining confidence in, individual privacy control can foster more cautious privacy behaviors on social media (Dienlin & Metzger, 2016; Epstein & Quinn, 2020). Research has found that people with higher formal education employ a variety of online privacy protection strategies more frequently, such as spam-filtering, changing passwords, and carefully looking at the addresses of emails they receive (Büchi et al., 2016; van Deursen & van Dijk, 2012).

Race is at the intersection of many social vulnerabilities (McDonald & Forte, 2022). In 2020, the poverty rates in the U.S. of Hispanics (17.0%) and African Americans (19.5%) were double that of non-Hispanic Whites (8.2%) and Asians (8.1%) (Shrider et al., 2021). There are also striking racial differences in educational attainment. In 2021, only 28.1% of African Americans and 20.6% of Hispanics reported having a Bachelor's degree or higher,

compared to 41.9% of non-Hispanic Whites and 61% of Asians (U.S. Census Bureau, 2022). A lack of educational and economic resources may inhibit access to training and tools that would help people navigate online privacy successfully. Indeed, African Americans and Latinos reported higher privacy concerns and feelings of vulnerability due to, for instance, fear of being unfairly targeted by law enforcement, compared to Whites (Auxier et al., 2019; Madden, 2017). Nonetheless, a recent literature review pointed out that race, as a central predictor of one's marginalization status, has received scant attention in the online privacy and marginalization literature (Sannon & Forte, 2022). Taken together, these results suggest that people who have more socioeconomic advantages (e.g., those with a college education, Whites, and Asians) may be better positioned to access and use essential resources for privacy management on social media. Therefore, this study conceptualizes marginalization status based on an individual's educational attainment (those without vs. with a college degree) and racial group (African Americans and Latinos vs. Whites and Asians).

To date, very few studies have empirically tested divides in online privacy *explicitly* on both the horizontal and vertical dimensions (Epstein & Quinn, 2020 is one exception), and most extant research in this realm examines internet privacy rather than social media privacy specifically. The following sections articulate rationales for educational and racial differences in privacy concerns and privacy management behaviors on social media.

Privacy Concerns on Social Media

Privacy concerns can be conceptualized as the degree to which social media users are concerned about the collection and use of their personal information by other users (i.e., horizontal concerns) and by institutions (i.e., vertical concerns) (Masur & Trepte, 2021). Compared to other online contexts such as e-commerce, social media provide a unique

situation in which individuals must simultaneously navigate both horizontal and vertical concerns, given the dynamics of information flow between different types of audiences. For example, when posting on Facebook, people may need to not only consider who in their friend networks may see their post, but also whether personal information contained in their post may be algorithmically added into their "digital trace profile" that may be further used for marketing or other purposes (Rice & Hoffman, 2018).

Past research has consistently pointed out that marginalized groups express higher levels of privacy concerns online (Madden, 2017), perhaps because they are more likely to have become the victims of online scams, abusive content, and blackmail (Büchi et al, 2021). Survey data show that overall, those without formal college education, African Americans, and Latinos expressed stronger privacy concerns than other groups about their privacy and data security on the Internet. For example, those without formal college education expressed privacy concerns about data breach (Cohn et al., 2020), identity theft, online scam or fraud (Madden, 2017), and online behavioral advertising (Smit et al., 2014). Similarly, African Americans and Latinos are strongly concerned about privacy violated by state and local government institutions and law enforcement (Auxier et al., 2019), being targeted in an online harassment (Madden, 2017), and consequences to privacy breach (Cohn et al., 2020). Although not explicitly studied, these concerns can be mapped to both the horizontal and vertical dimensions of privacy. Qualitative studies corroborate this pattern, finding that marginalized individuals expressed high (horizontal) privacy concerns about personal photos being stolen on social media (Bastick & Mallet-Garcia, 2022) and (vertical) concerns about policing surveillance as a result of structural racism (Marwick et al., 2017). Thus, the first set

of hypotheses aims to see if such online privacy divides can be replicated in the context of social media privacy on the horizontal and vertical privacy dimensions:

H1: People without a college degree will report higher (a) horizontal and (b) vertical privacy concerns on social media than those with a college degree.

H2: African Americans and Latinos will report higher (a) horizontal and (b) vertical privacy concerns on social media than Whites and Asians.

H3: Education and race will interact to impact privacy concerns such that African Americans and Latinos who do not have a college degree will report the highest (a) horizontal and (b) vertical privacy concerns on social media among all educational and racial groups.

Privacy Management Behaviors on Social Media

Privacy management behaviors can be understood as use of strategies to protect one's privacy online or on social media, and may occur on both the horizontal and vertical dimensions (Epstein & Quinn, 2020). Horizontal privacy management strategies are used to protect against user-to-user privacy incursions (e.g., limiting the visibility of certain posts to certain other individual social media users), while vertical strategies involve defending privacy invasions by institutional actors such as the government and corporations (e.g., turning off the personalized advertisement setting).

Research on divides in privacy management behaviors reveals mixed findings. On the one hand, survey data show that those with lower education, African Americans, and Latinos are less likely to indicate that they have used a range of horizontal and vertical strategies on the internet (e.g., blocking cookies), compared to other social groups (Büchi et al., 2021; Madden, 2017). This result is consistent with the digital divide perspective, which suggests

that a relative lack of resources and technical skills makes marginalized groups less likely to protect their privacy online, such as using services that allow people to browse the web anonymously (Madden, 2017), compared to non-marginalized groups. On the other hand, other research suggests that lack of trust in others and in institutions (discussed below) may create higher privacy concerns and motivate marginalized groups to take protection actions (e.g., keeping a low social media profile, abstaining entirely from social media) (Marwick et al., 2017; Smit et al., 2014; Vitak et al., 2018).

Yet, to my knowledge, only Epstein and Quinn (2020) have explicitly compared sociodemographic differences in the use of privacy management strategies based on the horizontal and vertical conceptual distinction. They found that age negatively predicted both horizontal and vertical privacy protection behaviors, and being female positively predicted horizontal protection behaviors but negatively predicted vertical protection behaviors. Although they found no differences by education or race, the extremely small sample sizes for racial minorities in their study does not allow for a meaningful comparison (African American, n = 59; Hispanic/ Latino, n = 53; Asian, n = 32; Caucasian, n = 564; multi-ethnic/other/undisclosed, n = 26). And their measures of vertical privacy management strategies examined internet privacy broadly (e.g., use of proxy server, encryption) that are less are less commonly used in the context of social media. Therefore, a larger and more balanced sample, particularly on parameters of education and race, and measures tailored towards *social media* privacy, are warranted to draw confident conclusions of divides in privacy management behaviors. Given the inconsistent evidence from the literature review above, the following research questions are posed:

RQ1: Does education impact the frequency of using (a) horizontal and (b) vertical privacy management strategies on social media?

RQ2: Does race impact the frequency of using (a) horizontal and (b) vertical privacy management strategies on social media?

RQ3: Do education and race interact to impact the frequency of using (a) horizontal and (b) vertical privacy management strategies on social media?

Theoretical Perspectives to Explaining the Online Privacy Divide

The final goal of this study is to advance a theoretically-informed explanation for the online privacy divide. The digital divide perspective is one common way to understand it (e.g., Büchi et al., 2021; Epstein & Quinn, 2020), which suggests that unequal distributions in access to digital technology and levels of digital skills due to socioeconomic and demographic differences (see van Dijk, 2020) may translate into corresponding inequalities in people's privacy experiences and skills online. For instance, research found that older, female (vs. male) identifying individuals, and those with lower education and lower-quality internet access have lower digital privacy and security skills, and are less likely to engage in preventive anti-virus behaviors (Dodel & Mesch, 2018; Li et al., 2018). Madden (2017) similarly found that those without a college degree and foreign-born Hispanic internet users were among the least likely to use privacy management strategies online, compared to other educational and racial groups. This makes sense given that a lack of access to reliable digital technology may limit individuals' internet experience and further inhibit the development of basic digital privacy skills.

In contrast, a handful of qualitative studies suggest that marginalized groups have high awareness of privacy risks and are very active in protecting their privacy online (e.g.,

Marwick et al., 2017; Vitak et al., 2018). A dive into these studies suggests that *trust* may be a key factor that motivates privacy protection behaviors of the marginalized groups. For example, in an interview study with self-identified low-income, immigrant, sexual or racial minority individuals, Marwick and colleagues (2017) found that traumatizing physical surveillance and police harassment experiences may have contributed to participants' overall lack of trust in other people and institutions. A number of participants reported refraining from many online activities as a means to minimize perceived privacy threats posted by employers and government online surveillance. Similarly, Vitak and colleagues (2018) found that individuals who live in high poverty and low education communities tended to distrust and even fear online services and digital technologies, and thus were likely to reject online job applications and banking services to prevent violation of privacy online.

Although the digital skills perspective has been primarily adopted to explain divides in online privacy management (e.g., Büchi et al., 2021, Li et al., 2018), virtually no studies have quantitatively examined the role that trust plays in explaining such divides. Yet discrimination and victimization experienced by marginalized individuals may suppress their propensity to trust other people and institutions (e.g., the government, corporations, and social media platforms) (Best et al., 2021; Smith, 2010; Pearce & Rice, 2017), which may in turn lead to higher privacy concerns and motivate privacy protection (e.g., Marwick et al., 2017).

The Important Role of Trust in Online Privacy

Trust is long recognized as playing an important role in online privacy and self-disclosure. Trust is a central motivation for people to reveal personally-identifiable information on social media because it ameliorates one's concerns about potential privacy

risks (Krasnova et al., 2010; Mesch, 2012). It is associated with lower online privacy concerns and higher willingness to disclose personal information in various contexts (Baik & Jang, 2022; Joinson et al., 2010).

Marginalized groups, particularly African Americans and Latinos, report lower levels of various types of trust (Douds & Wu, 2017; Wilkes & Wu, 2019), as they disproportionately experience discrimination in both everyday social interactions and in institutional settings such as housing, employment, and policing (Pager & Shepherd, 2008). Such attitudes may be socialized, for example, through vicarious experiences of racism, or the indirect knowledge of racial oppression that children learn through socialization with other people, especially parents, which can contribute to an overall lack of trust (Evangelist, 2022). Research also shows that African Americans and Hispanics hold lower levels of trust towards doctors and healthcare institutions due to historical experiences of being victimized in medical settings (Richardson et al., 2012; Williamson, 2021).

A lower level of trust may impact marginalized groups' online privacy concerns and privacy management behaviors because it underlies perceived privacy risks and alerts people in a way that may prompt them to more cautiously manage personal information. On the horizontal dimension of privacy, marginalized groups may be concerned about other individuals (i.e., employers, doxxers) violating their privacy due to low levels trust in other people (i.e., generalized social trust), whereas on the vertical dimension they may protect their privacy because they do not trust the intentions of the institutions that may collect their data online (e.g., the government, law enforcements). Therefore, this study conceptualizes trust in terms of both generalized social trust and institutional trust to reflect the privacy

risks, respectively, on the horizontal and vertical dimensions of privacy posed by the different entities that may have access to social media users' personal information.

Generalized Social Trust

Generalized social trust is the perception that most people that we have no previous information about can be trusted (Dinesen, 2012), and is developed primarily based on past and present interpersonal experiences (Twenge et al., 2014). Breham and Rahn (1997) argue that being a member of marginalized groups increases the likelihood of witnessing instances of discrimination and prejudice, which may lead to suspiciousness of one's surroundings and the motives of others, and hence lower generalized social trust.

Nationally representative surveys show that generalized social trust differs by education and race in the U.S. Taylor and colleagues (2007) found the percentage of "high trusters" in the White population was double that of African Americans and Hispanics: whereas 27% of Whites reported a high level of trust, only 13% of African Americans and 12% of Hispanics did so. Similarly, 50% of college graduates were "high trusters," compared with only 28% of those with a high school degree or less. Lower generalized trust may cause people to be suspicious of the motives of other social media users online, and perhaps more cautious of revealing one's own personal information on social media.

Further, research found that racially marginalized groups who have low levels of generalized social trust tend to engage in less online networking activities to minimize the privacy risks of disclosing personal information on the horizontal privacy dimension. For instance, Gonzales and colleagues (2021), in their qualitative study, suggested that trust may moderate marginalized groups' intention to reach out to unfamiliar sources online for professional networking purposes. In particular, African Americans and Latinos exhibited a

lack of trust in others as a result of previous negative experiences online, and thus were more likely to limit their contacts to vetted existing networks, whereas low-income Whites who rarely mentioned trust issues had more conversations with strangers online. Research also found that, due to a lack of trust in others, racially marginalized and low-income individuals tend to hesitate to seek out strangers in online communities for informational and emotional support (Hui et al., 2023; Israni et al., 2021), and may intentionally not post social media content that can be later identified by unintended users, such as their employers (Marwick et al., 2017). Therefore, generalized social trust may explain, via mediation, the impacts of education and race on horizontal privacy concerns (H4) and privacy management behaviors (H5).

> H4: Generalized social trust will mediate the impacts of education and race on horizontal privacy concerns on social media, such that (a) people without a college degree and (b) African Americans and Latinos will report lower social trust, which will predict higher horizontal concerns, compared to people with a college degree and Whites and Asians.
>
> H5: Generalized social trust will mediate the impacts of education and race on the frequency of using horizontal privacy management strategies, such that (a) people without a college degree and (b) African Americans and Latinos will report lower generalized social trust, which will predict higher frequency of using horizontal strategies, compared to people with a college degree and Whites and Asians.

Institutional trust

Levels of generalized social trust are distinct from, yet often positively correlated with, levels of institutional trust (Rainie et al., 2019), which may impact people's concerns

and management behaviors on the vertical dimension of privacy. Institutional trust can be understood as an individual's expectation and confidence that a given institution will produce positive outcomes toward oneself or others (Levi & Stoker, 2000). It is closely tied to an individual's perceptions of credibility, fairness, competence, and transparency of a given institution (Sønderskov & Dinesen, 2016). Survey results show that people without a college degree have lower trust towards internet service and cell phone providers in their ability to keep users' personal information safe, compared with people who have a formal education (Madden, 2017). Likewise, African Americans and foreign-born Hispanics are considerably less trusting of law enforcement than Whites and U.S.-born Hispanics (Madden, 2017; Redmiles & Buntain, 2021). And in a health context, African Americans were more likely than their White counterparts to bring up mistrust of the government and medical institutions when asked about their attitudes towards vaccines because they were historically treated unfairly by the medical establishment (Jamison et al., 2019; Williamson, 2021).

Indeed, negative past experiences that marginalized groups have had may impact their trust in various institutions (e.g., government agencies, corporations, advertisers, law enforcement), which may in turn shape their vertical privacy concerns and behaviors. For example, African Americans are reluctant to share personal health information, such as health symptoms and lab results, with providers online (Graham & Smith, 2018), suggesting a lack of trust in eHealth systems. Fear of surveillance stemming from interpersonal experiences and media coverage promoted low-income Latino parents to enact privacy monitoring strategies (e.g., installing content-blocking systems, reviewing browser caches) to prevent their children's oversharing online (Katz & Gonzalez, 2016). People with lower institutional trust may less frequently participate in social media activities that require

personal information, such as signing petitions for political events, to avoid being tracked by the government and other entities (Lutz & Hoffmann, 2021). Trust in governments was also found to negatively predict online privacy concerns associated with government surveillance (Männiste & Masso, 2018) and to positively predict tolerance towards state dataveillance (Kalmus et al., 2022). Thus, differences in institutional trust may further explain divides in vertical privacy concerns (H6) and vertical privacy management behaviors (H7).

H6: Institutional trust will mediate the impacts of education and race on vertical privacy concerns on social media, such that (a) people without a college degree and (b) African Americans and Latinos will report lower institutional trust, which will predict higher vertical concerns, compared to people with a college degree and Whites and Asians.

H7: Institutional trust will mediate the impacts of education and race on the frequency of using vertical privacy management strategies, such that (a) people without a college degree and (b) African Americans and Latinos will report lower institutional trust, which will predict higher frequency of using vertical strategies, compared to people with a college degree and Whites and Asians.

Method

Recruitment Procedure

Upon IRB approval, an online survey was administered between February and April, 2023 through Qualtrics XM's Research Panel. The incentives were based on the amount of time required to complete the survey (M = 17.50 minutes) and the sources from which participants were recruited by Qualtrics to their panels. In other words, when participants were invited to take the survey, they were informed what they would be compensated for.

For example, participants could be airline customers who could choose SkyMiles for their reward, retail customers who opted into the survey could opt to get points at their favorite retail outlet, or general consumers could choose to participate for cash or gift cards, etc. Participants were also informed in the consent form "you will be compensated the amount you agreed upon before you entered into the survey."

2020 census data show the following racial breakdown in terms of percentages of the U.S. population: Non-Hispanic white (61.6%), Hispanic (48.0%), African American (12.4%) and Asian (6.0%). Consequently, random sampling from the population would require a very large, and thus very expensive, sample. Given the comparative aims of this research, purposive sampling was employed to recruit an approximately equal number of participants on the parameters of education and race among members of the U.S. population, resulting in four groups: (1) African Americans and/or Latinos without a college degree, (2) African Americans and/or Latinos with a college degree, (3) Whites and/or Asians without a college degree, and (4) Whites and/or Asians with a college degree. Within each of these four groups, I also sought to recruit a roughly equal number of participants for each racial group (e.g., African Americans (50%) and/or Latinos (50%) without a college degree).

To ensure data quality, several screening criteria were added to the survey, such that participants had to be a social media user (i.e., have at least one social media account and have experiences using social media) and indicate their commitment to providing thoughtful answers to the survey questions. Participants who sped through or completed the survey in under five minutes, failed the attention check, and straight-lined the survey were excluded from the final dataset by Qualtrics' data scrubbing team. Qualtrics recruited and replaced

these participants in the dataset with other participants who met the data quality requirements.

Sample

An a priori power analysis using G*Power 3.1 suggested that a total sample size of *N* = 1302 was needed to test the hypotheses of this study with the smallest effect size of interest (*f* = .1), a power of 95%, and the usual alpha level of 5%. The final dataset included a total of 1401 responses: (1) African Americans and/or Latinos without a college degree (*N* = 343), (2) African Americans and/or Latinos with a college degree (*N* = 355), (3) Whites and/or Asians without a college degree (*N* = 348), and (4) Whites and/or Asians with a college degree (*N* = 355). Across the entire sample, 60.5% (*N* = 848) were female, 39.0% (*N* = 547) were male, and .4% (*N* = 6) were non-binary. The average age was 41.35 years old (*SD* = 16.44, range = 18-101), and the average annual income was between $55,000 and $60,000 (range = under $5,000- $200,000 and over). Education and race were measured (see Appendix A) and coded based on the conceptualization of marginalized status. Thus, for education, 49.3% (*N* = 691) of the participants were coded as having no college degree and 50.2% (*N* = 710) as having a college degree. The final racial composition included 49.8% racially marginalized individuals (i.e., African Americans and Latinos) (*N* = 698) and 50.2% racially non-marginalized (i.e., Whites and Asians) individuals (*N* = 703).

Measures

Consistent with the conceptualizations discussed earlier, key variables were operationalized based on the horizontal and vertical distinctions of privacy (see Appendix B for a list of all measures and items, as well as means and standard deviations for each item and their mean scales). Question stems were developed to prime participants to reflect on

privacy experiences vis-à-vis different audiences on social media. For example, the horizontal privacy measures ask participants to think about friends, family members, coworkers, employers, strangers, and other individual social media users that may have access to their personal information on social media, whereas the vertical privacy measures emphasize government agencies, social media companies, advertisers, corporations, and other organizations as the potential audiences.

Privacy Concerns

Participants reported privacy concerns on a 7-point Likert scale ranging from 1 = strongly disagree to 7 = strongly agree. Ten horizontal concern items were adapted from existing scales (Krasnova et al., 2009), such as "I am concerned that I don't have control over what other users do with information I post on social media." Seven vertical concern items were adapted from prior research (Auxier et al., 2019; Dinev et al., 2008; Krasnova et al., 2009) and included items that can specifically capture marginalized groups' privacy concerns. For example, "I am concerned that the power the government and law enforcement have to wiretap my social media activities might threaten the safety of me and my family." Cronbach's alpha reliability coefficient was .86 for the horizontal concern scale, and .84 for the vertical concern scale.

Privacy Management Behaviors

Privacy management behaviors included eight horizontal privacy management strategies and seven vertical strategies. Participants indicated the frequency of using these strategies on a 5-point Likert scale ranging from 1 = never to 5 = always. Horizontal strategies were adapted from Wang and Metzger (2021), such as blocking certain contacts or creating a fake account. Most existing scales on vertical strategies focus on internet privacy

(e.g., use VPN, delete cookies) that are not applicable in the social media context. In addition, existing scales on privacy management have also been criticized for not capturing a wide range of strategies, thus ignoring the nuances in skills inequality (Chen & Li, 2022). The current vertical strategies scale is inspired by prior instruments (Hoy & Milne, 2010; Min, 2019), supplemented with findings of qualitative studies that shed light on marginalized individuals' privacy management on social media (e.g., avoid posting information that may be seen as problematic by government agencies or law enforcement if they monitor my social media accounts) (Marwick et al., 2017; Walker & Hargittai, 2021). Cronbach's alpha was .88 for the horizontal privacy management strategies, and.85 for the vertical strategies scale.

Generalized Social Trust

Although commonly used to measure generalized social trust, Rosenberg's (1956) misanthropy scale has been criticized for its dichotomized items, which decrease the detail in which latent factors can be measured (Krosnick & Fabrigar, 1997; Lundmark et al., 2016). Research has demonstrated that increasing the number of scale points can produce a more valid measure of generalized social trust (Krosnick & Fabrigar, 1997; Lundmark et al., 2016, Zmerli & Newton, 2008). In addition, breaking the lengthy polarized statements (e.g., "most people can be trusted or you need to be very careful in dealing with people") into single viewpoint statements (e.g., "most people can be trusted" and "you need to be very careful in dealing with people") minimizes the task difficulty and increases the validity of the measurement (Lundmark et al., 2016). Following these suggestions, the three original dichotomous generalized social trust statements were transformed into six items, measured on a 7-point scale (1 = strongly disagree; 7 = strongly agree). Cronbach's alpha was .77.

Institutional Trust

Adapted from Liu et al. (2018), the institutional trust scale assessed the degree to which participants trusted different institutions on a 7-point scale (1 = do not trust at all, 7 = trust completely). A battery of 13 institutions that may impact social media users' privacy experiences were presented based on previous research (Betts, 2020; Madden, 2017; Pearce & Rice, 2017). Examples include the US judicial (court) system, police and other law enforcement agencies, and social media companies. Cronbach's alpha was .93.

Sociodemographic Variables

As described above, participants self-reported their race/ethnicity, education levels, income, sex/gender identity, and age. In addition, street race was measured by asking participants "If you were walking down the street, what race do you think other Americans who do not know you personally would assume you were based on what you look like? (select one)" (López et al., 2018). Therefore, participants who did not identify with one of the four racial groups of interest were recoded based on their street race. Education and race were recoded into dichotomous variables, consistent with this study's conceptualization of marginalized status. As such, African Americans and Latinos were coded as marginalized groups (0) and Whites and Asians as non-marginalized groups (1). Likewise, those without a college degree were coded as 0, and those with a college degree were coded as 1.

Control Variables

Previous online privacy violation experiences were measured by asking participants if they or people close to them ever had a negative privacy experience on social media (e.g., been a victim of an online scam, had personal information stolen) (Metzger & Suh, 2017).

Frequency of social media update was measured by asking participants how often they add new content to their social media accounts (e.g., posts, stories).

Results

Privacy Concerns

Hypotheses 1-3 predicted main effects for education (H1), race (H2), and interaction effects of education and race (H3) on (a) horizontal and (b) vertical privacy concerns. To test these hypotheses, a two-way Analysis of Covariance (ANCOVA) was conducted with education (i.e., without vs. with a college degree), race (i.e., African Americans and Latinos vs. Whites and Asians), as well as their interaction, as the predictor variables and horizontal privacy concerns as the outcome variable, controlling for previous privacy violation experiences and social media update frequency. The same analysis was then conducted with vertical privacy concerns as the outcome variable.

H1 predicted that people without a college degree would report higher (a) horizontal and (b) vertical privacy concerns on social media than those with a college degree. The analysis revealed a significant main effect for education on horizontal privacy concerns, $F(1, 1395) = 22.91$, $p < .001$, $\eta_p^2 = .02$, and vertical privacy concerns, $F(1, 1395) = 8.07$, $p < .01$, $\eta_p^2 = .01$. People without a college degree reported significantly lower horizontal and vertical privacy concerns ($M_{Horizontal} = 4.31$, $SE = .04$; $M_{Vertical} = 4.57$, $SE = .05$) than people with a college degree ($M_{Horizontal} = 4.60$, $SE = .04$; $M_{Vertical} = 4.72$, $SE = .05$). Thus Hypothesis 1 was not supported.

H2 predicted that African Americans and Latinos would report higher (a) horizontal and (b) vertical privacy concerns on social media than Whites and Asians. No significant

main effect was found for race on horizontal, $F(1, 1395) = 2.42$, $p = .12$ or vertical privacy concerns, $F(1, 1395) = .01$, $p = .93$. Hypothesis 2 was not supported.

H3 predicted an interaction effect of education and race, such that African Americans and Latinos who do not have a college degree would report the highest (a) horizontal and (b) vertical privacy concerns among all educational and racial groups. The omnibus tests were not significant for horizontal concerns, $F(1, 1395) = 1.57$, $p = .21$, $\eta_p^2 = .00$, and only approached significance for vertical concerns, $F(1, 1395) = 3.63$, $p = .06$, $\eta_p^2 = .00$, suggesting no significant interaction of education and race on privacy concerns. Hypothesis 3 was not supported.

Privacy Management Behaviors

Research questions 1-3 asked if there are main effects for education (RQ1), race (RQ2), and their interactions (RQ3) on the frequency of using (a) horizontal and (b) vertical privacy management strategies on social media. To answer these questions, a two-way ANCOVA was conducted with education and race, as well as their interaction, as the predictor variables and use of horizontal privacy management strategies as the outcome variable, controlling for previous privacy violation experiences and social media update frequency. The same analysis was then conducted with vertical privacy management strategies use frequency as the outcome variable.

RQ1 asked if education impacts the frequency of using (a) horizontal and (b) vertical privacy management strategies on social media. The main effects of education were not significant on frequency of using horizontal strategies, $F(1, 1374) = .49$, $p = .48$, $\eta_p^2 = .00$, and vertical privacy strategies, $F(1, 1380) = 1.80$, $p = .18$, $\eta_p^2 = .00$. RQ2 asked if race is associated with the frequency of using (a) horizontal and (b) vertical privacy management

strategies on social media. The analysis revealed a significant main effect for race on frequency of using horizontal strategies, $F(1, 1374) = 21.25$, $p < .001$, $\eta_p^2 = .02$, and vertical strategies, $F(1, 1380) = .11.24$, $p < .001$, $\eta_p^2 = .01$. African Americans and Latinos reported significantly higher frequency of using horizontal and vertical privacy management strategies ($M_{Horizontal} = 2.53$, $SE = .04$; $M_{Vertical} = 2.54$, $SE = .04$) than Whites and Asians ($M_{Horizontal} = 2.30$, $SE = .04$; $M_{Vertical} = 2.37$, $SE = .04$).

RQ3 asked if education and race interact to impact the frequencies of using (a) horizontal and (b) vertical privacy management strategies. The omnibus tests were not significant for horizontal privacy strategies use, $F(1, 1374) = 2.13$, $p = .15$, $\eta_p^2 = .00$, or for vertical privacy strategies use, $F(1, 1380) = 1.61$, $p = .21$, $\eta_p^2 = .00$, suggesting no significant interaction of education and race on privacy management behaviors.

Generalized Social Trust

H4 through H7 predicted that generalized social trust and institutional trust would mediate the impact of education and race on privacy concerns and privacy management behaviors. A series of mediation analyses were conducted using Hayes' PROCESS (Model 4), while controlling for previous privacy violation experiences and social media update frequency.

H4 predicted that generalized social trust would mediate the effects of (a) education and (b) race on horizontal privacy concerns. For education (see Figure 1), people without a college degree reported significantly lower horizontal concerns, $b = .29$, $t(1397) = 4.78$, $p < .001$, and lower generalized social trust, $b = .26$, $t(1397) = 5.02$, $p < .001$, than people with a college degree. Generalized social trust, in turn, negatively predicted horizontal concerns, $b = -.08$, $t(1396) = -2.60$, $p < .01$. In addition, the model indicated a significant indirect effect of

education on horizontal concerns via generalized social trust with a bootstrap sample of 5,000 samples and 95% confidence interval, b = -.02, SE = .01, CI[-.04, -.00], such that compared to people with a college degree, those without a college degree reported lower social trust, which led to higher horizontal concerns. The direct impact of education on horizontal concerns, controlling for the impact of generalized social trust, remained significant, b = .31, t(1396) = 5.09, p < .001. Therefore, generalized social trust partially mediated the impact of education on horizontal concerns, supporting H4a.

For race (see Figure 2), no significant impact of race was found on horizontal concerns, b = .10, t(1397) = 1.57, p = .12. However, African Americans and Latinos reported significantly lower generalized social trust than Whites and Asians, b = .18, t(1397) = 3.52, p < .001. Generalized social trust, in turn, negatively predicted horizontal concerns, b = -.07, t(1396) = -2.08, p < .05. Finally, the model indicated no significant indirect effect of race on horizontal concerns via generalized social trust with a bootstrap sample of 5,000 samples and 95% confidence interval, b = -.01, SE = .01, CI[-.03, .00]. Therefore, H4b was not supported.

H5 predicted that generalized social trust would mediate the effects of (a) education and (b) race on the frequencies of using horizontal privacy management strategies. For education (see Figure 3), no significant impact of education was found on the frequency of using horizontal strategies, b = .03, t(1376) = .63, p = .53. However, people without a college degree reported significantly lower generalized social trust than people with a college degree, b = .26, t(1376) = 5.09, p < .001. Generalized social trust, in turn, negatively predicted horizontal strategies use, b = -.05, t(1375) = -2.06, p < .05. In addition, the model indicated a significant indirect effect of education on horizontal strategies use via generalized social trust with a bootstrap sample of 5,000 samples and 95% confidence interval, b = -.01, SE = .01,

CI[-.03, -.00], such that compared to people with a college degree, those without a college degree reported significantly lower generalized social trust, which predicted higher frequency of using horizontal strategies. Therefore, generalized social trust mediated the impact of education on horizontal strategies use, supporting H5a.

For race (see Figure 4), African Americans and Latinos reported a significantly higher frequency of using horizontal strategies, b = -.23, t(1376) = -4.59, p < .001, and lower generalized social trust, b = .19, t(1376) = 3.53, p < .001, than Whites and Asians. However, generalized social trust did not predict horizontal strategies use, b = -.04, t(1375) = -1.54, p = .12. Further, no significant indirect effect of race was found on horizontal strategies use via generalized social trust with a bootstrap sample of 5,000 samples and 95% confidence interval, b = -.01, SE = .01, CI[-.02, .00]. Therefore, H5b was not supported.

Institutional Trust

H6 predicted that institutional trust would mediate the effects of (a) education and (b) race on vertical privacy concerns. For education (see Figure 5), people without a college degree reported significantly lower vertical concerns, b = .18, t(1397) = 2.83, p < .01, and lower institutional trust, b = .27, t(1397) = 4.41, p < .001, than people with a college degree. Institutional trust, in turn, negatively predicted vertical concerns, b = -.12, t(1396) = -4.32, p < .001. In addition, the model indicated a significant indirect effect of education on vertical concerns via institutional trust with a bootstrap sample of 5,000 samples and 95% confidence interval, b = -.03, SE = .01, CI[-.06, -.01], such that compared to people with a college degree, those without a college degree reported lower institutional trust, which led to higher vertical concerns. The direct impact of education on vertical concerns, controlling for the impact of institutional trust, remained significant, b = .22, t(1396) = 3.33, p < .001.

Therefore, institutional trust partially mediated the impact of education on vertical concerns, supporting H6a.

For race (see Figure 6), no significant impact of race on vertical concerns was found, $b = .01$, $t(1397) = .12$, $p = .91$. However, African Americans and Latinos reported significantly lower institutional trust than Whites and Asians, $b = .01$, $t(1397) = .12$, $p < .001$. Institutional trust, in turn, negatively predicted vertical concerns, $b = -.11$, $t(1396) = -3.96$, $p < .001$. In addition, the model indicated a significant indirect effect of race on vertical concerns via institutional trust with a bootstrap sample of 5,000 samples and 95% confidence interval, $b = -.02$, $SE = .01$, CI[-.04, -.01], such that compared to Whites and Asians, African Americans and Latinos reported lower institutional trust, which predicted higher vertical concerns. Therefore, institutional trust mediated the impact of race on vertical concerns, supporting H6b.

H7 predicted that institutional trust would mediate the effects of (a) education and (b) race on the frequency of using vertical privacy management strategies. For education (see Figure 7), no significant impact of education was found on the frequency of using vertical strategies, $b = .07$, $t(1382) = 1.32$, $p = .19$. However, people without a college degree reported significantly lower institutional trust, $b = .28$, $t(1382) = 4.53$, $p < .001$, than people with a college degree. Institutional trust only marginally predicted vertical concerns, $b = .04$, $t(1381) = 1.82$, $p = .07$. Further, no significant indirect effect of education was found on vertical strategies use frequency via institutional trust with a bootstrap sample of 5,000 samples and 95% confidence interval, $b = .01$, $SE = .01$, CI[-.00, .03]. Therefore, H7a was not supported.

For race (see Figure 8), African Americans and Latinos reported significantly higher frequency of using vertical strategies, b = -.17, t(1382) = -3.34, p < .001, and lower institutional trust, b = .20, t(1382) = 3.20, p < .01, than Whites and Asians. Institutional trust, contrary to prediction, positively predicted vertical strategies use, b = .05, t(1381) =2.27, p < .05. Further, the model indicated a significant indirect effect of race on vertical strategies use via institutional trust with a bootstrap sample of 5,000 samples and 95% confidence interval, b = .01, SE = .01, CI[.00, .02], such that compared to Whites and Asians, African Americans and Latinos reported significantly lower institutional trust, which predicted lower frequency of using vertical strategies. The direct impact of race on vertical strategies use frequency, controlling for the impact of institutional trust, remained significant, b = -.18, t(1381) = -3.52, p < .001. Therefore, because the observed partial mediation suggested a different pattern than what was hypothesized, H7b was not supported.

Summary

In sum, in some cases the results support the hypotheses proposed and theoretical arguments advanced but not in all cases. Generally speaking, the data lend more support to the meditation hypotheses than to the other types of hypotheses. See Table 2 for a summary of results.

Discussion

General Discussion

Questions have been raised regarding whether an online privacy divide exists between people from different social backgrounds (e.g., Epstein & Quinn, 2020). This study attempts to answer this question by quantitatively examining such divides by education and race in both privacy concerns and privacy management behaviors on social media.

Additionally, it examines a previously overlooked explanation for such divides. Whereas the digital divide literature proposes that privacy divide is due to differences in technological resources and privacy training, this study examines the role of social and institutional trust in creating a privacy digital divide.

Evidence for an Online Privacy Divide?

Differences in education (without vs. with a college degree) and race (African Americans and Latinos vs. Whites and Asians) were explored with regard to privacy concerns (H1-H3) and privacy management behaviors (RQ1-RQ3) on both the horizontal and vertical dimensions of privacy. H1-H2 predicted that marginalized groups would report higher privacy concerns, as consistently pointed out by previous research (Auxier et al., 2019; Cohn et al., 2020; Madden, 2017). Yet this study found the opposite for education, such that people without a college degree reported lower privacy concerns on both the horizontal and vertical dimensions of privacy compared to those with a college degree. This lends support to the digital divide perspective, which suggests that due to lack of access to technological devices and relevant privacy literacy training and privacy management resources, less educated individuals are less likely to realize the issue severity and potential risks of online privacy. Moreover, in contrast to the prediction, no main effect was found for race. An inspection of the mean scores indicated that Africans Americans and Latinos ($M_{Horizontal}$ = 4.41, $M_{Vertical}$ = 4.66) as well as Whites and Asians ($M_{Horizontal}$ = 4.50, $M_{Vertical}$= 4.66) reported overall very high privacy concerns. This result warrants more investigation, as although privacy issues seem to engender universal concerns across racial groups, reasons that explain these privacy concerns may be different for different populations. For example,

marginalized groups may be concerned about privacy due to a lack of trust, while non-marginalized groups may be concerned mainly because of previous violation experiences.

RQ1-RQ2 asked about whether marginalized groups would employ privacy management strategies more frequently than non-marginalized groups. One notable finding of this study is that racially marginalized groups (i.e., African Americans and Latinos) reported using privacy management strategies *more frequently* than non-marginalized groups (i.e., Whites and Asians) on both the horizontal and vertical dimensions of privacy. This finding challenges the assumptions of prior studies based on the digital divide perspective that marginalized groups are less able to protect their online privacy due to lack of resources and skills (Büchi et al., 2021; Madden, 2017). Rather, this finding quantitatively supports results of qualitative studies that found marginalized groups *more* actively employ a variety of strategies to protect their online privacy, perhaps because of greater privacy threat perceptions (Marwick et al., 2017; Vitak et al., 2018).

No main effect was found for education, but as mentioned earlier, existing measures of privacy management have been criticized for not including a wide range of strategies employed by people from different sociodemographic backgrounds (Chen & Li, 2022). The fact that privacy strategies that are commonly used by marginalized individuals (e.g., avoiding posting problematic comments, leaving social media), suggested by qualitative research, were included in the measures in this study may explain why the results differ from previous research. In any case, the result for RQ1 suggests that regardless of one's education, people find their way to manage social media privacy. Future research may attempt to uncover latent classes of privacy management strategies predicted by group memberships, perhaps by leveraging mixture modeling techniques. Indeed, if non-use is the major privacy

management strategy that marginalized groups tend to use, implications on how much they are able to reap rewards and social capital from social media warrants more attention.

H3 and RQ3 speculated that individuals who are both educationally and racially marginalized (i.e., highest level of marginalization) would report the highest privacy concerns and protect their privacy the most frequently. Yet none of the interactions of education and race were significant. This suggests the need to test alternative predictors of marginalization, alongside standard sociodemographic variables. Indeed, based on the reviewed literature that argues actual or perceived discrimination experiences of marginalized groups may exacerbate their online privacy concerns (e.g., Marwick et al., 2017), it is possible that *perceived marginalization* (i.e., subjective experiences and feelings of being marginalized and discriminated), regardless of one's educational and racial groups, better predicts online privacy outcomes than standard sociodemographic variables that typically serve as proxies for marginalization.

This study also advanced and tested generalized social trust (H4-H5) and institutional trust (H6-H7) as explanatory mechanisms for the online privacy divide. Results revealed some interesting patterns on privacy concerns. In particular, although people without a college degree were found to have low horizontal and vertical concerns in the main effects tests, generalized social trust and institutional trust acted as *suppressor* variables in the mediation models such that because people without a college degree had low trust, this in turn led to higher privacy concerns. This finding further demonstrates the importance of considering how lived experiences of marginalized groups may shape their privacy attitudes on social media. On the surface, results of main effects suggest less educated individuals are less literate of privacy risks on social media. But adding trust into the model delineates a

fuller picture and reveals that a lack of trust, in fact, led less educated individuals to be *more* alert of privacy issues on social media.

A similar pattern also occurred for race, such that African Americans and Latinos reported higher vertical concerns *only through* lower institutional trust, compared to Whites and Asians. On the horizontal dimension, however, although African Americans and Latinos reported lower generalized social trust, which negatively predicted horizontal concerns, the indirect effect was not significant. Considering that no main effect was found for race on privacy concerns, future research is warranted to probe factors or processes that contribute to racially marginalized groups' privacy concerns. One possibility is that these groups perceived high benefits of social media self-disclosure (e.g., capital building, relational maintenance) on the horizontal dimension of privacy, which in turn, undermined their privacy concerns. Nonetheless, these results continue to reinforce the critical role of trust in privacy and marginalization.

Results on privacy management behaviors revealed mixed patterns. Although no main effect was found for education in the ANCOVA analyses, generalized social trust mediated its impact on the use of horizontal strategies, such that people without a college degree use horizontal privacy strategies more frequently than people with a college degree, through reduced social trust. Contrary to the prediction, while African Americans and Latinos reported significantly lower institutional trust, this led to *lower* frequency of using vertical strategies, compared to Whites and Asians. While no easy explanation for this finding presents itself, one possibility is that low institutional trust as a result of structural racism might lead marginalized groups to lose privacy self-efficacy and thus the motivation to engage in any privacy management behaviors. The concept of privacy cynicism, defined

as feelings of uncertainty, mistrust, and powerlessness towards the collection and processing of personal data by institutions online (e.g., organizations, advertisers, governments), can help illustrate such a tendency to engage in less privacy protection, specifically on the vertical privacy dimension (Hoffmann et al., 2016; van Ooijen et al., 2022). It is possible that marginalized groups may experience a stronger sense of privacy cynicism on social media. Regardless, future research is warranted to further unpack the nuances in how different racial groups respond to and manage privacy issues on social media.

Finally, social trust did not mediate the impact of race on privacy management, and institutional trust did not mediate the impact of education on privacy management. It is possible that although lack of trust may increase marginalized individuals' privacy concerns, it does not always drive their privacy management behaviors by itself. Protection management theory (Maddux & Rogers, 1983; Rogers, 1975) may suggest that the way people appraise social media privacy (e.g., perceived vulnerability, privacy self-efficacy, response efficacy) could explain divides in management behaviors. For example, privacy self-efficacy may positively predict privacy management behaviors, and education and race may moderate this relationship. These should be tested in future research.

In summary, overall the results of this study reveal some empirical evidence of an online privacy divide by education and race, demonstrate how trust attitudes held by marginalized groups (especially less educated individuals) as a result of their lived experiences impact privacy concerns and privacy management behaviors, and underscore the need for more research to further understand the nuanced impact of marginalization on online privacy management.

Theoretical and Practical Contributions

Drawing from the integrated model of online privacy (Bazarova & Masur, 2020), this study set out to discover if empirical evidence for a potential online privacy divide could be found, to test trust as the mediating mechanism for such a divide, to elaborate Bazarova and Masur's theoretical framework, and to add to the scant extant research on online privacy and marginalization.

To my knowledge, this study is not only the first to empirically test the integrated model of online privacy and its horizontal and vertical privacy conceptual distinction (Bazarova & Masur, 2020), but is also the first to advance the model by proposing and testing generalized social trust and institutional trust as important components to understand privacy attitudes and behavior within a sociodemographically diverse sample. Results demonstrate that education and race impact privacy *differently* on the horizontal and vertical dimensions of privacy, thereby confirming the importance of such conceptual distinctions. For instance, although trust mediated the impact of race on vertical privacy concerns, this was not the case on the horizontal dimension. Indeed, privacy scholars have been imploring researchers to consider the conceptual and operational nuances of online privacy-related phenomena, including different forms and dimensions of privacy (e.g., Dienlin & Trepte, 2015; Masur, 2018, 2021). The horizontal and vertical distinction could be utilized to further elaborate and test the robustness of existing privacy theories, such as the privacy calculus (Dienlin & Metzger, 2016; Laufer & Wolfe, 1977). For example, do privacy calculus components, such as perceived benefits, privacy concerns, and privacy self-efficacy predict privacy management behaviors on both the horizontal and vertical dimensions of privacy? Given that people often have little control over vertical privacy (Hoffmann et al., 2016; van

Ooijen et al., 2022), would there be any evidence for a privacy paradox (i.e., a non-significant relationship between privacy concerns and privacy management behaviors) specifically on the vertical dimension of privacy? Further, how might these relationships differ for people from different sociodemographic backgrounds?

Perhaps most noteworthy, results of this study lend some initial support to the proposed notion of an *online privacy divide*, which argues that structural racism and discrimination experiences of marginalized individuals will manifest in online privacy attitudes and behaviors through different types of trust, along with traditional markers of marginalization (e.g., digital access, skills). As such, the *online privacy divide* echoes Park's (2021) argument of the social construction of privacy and relies on both the digital divide and the trust literatures to emphasize the complex relationship between privacy and marginalization that looks beyond the individual level to consider how lived experiences of marginalized groups may shape their online privacy outcomes. A theoretical framework that may usefully guide future privacy research is Bronfenbrenner's (1979) ecological systems theory that studies individuals in networked ecological systems. Applied to the online privacy divide, factors at different social ecological levels may independently and/or interactively shape marginalized groups' privacy attitudes and behaviors, such as individual- (e.g., SES, gender, age), meso- (e.g., parents, peers), exo- (e.g., neighbors, politics, mass media), and macro- levels (e.g., culture, attitudes, values). For example, a lack of trust toward government cultivated by family members may be reinforced by mass media reports and policy making (e.g., Stop-and-Frisk), which may further impact how marginalized individuals think about and manage vertical privacy online.

Practically, findings of the present study reveal the need for continued effort for privacy education, especially targeting less educated social media users. As technology almost becomes a default for participating in several aspects of contemporary society, such as health, employment, and politics, it is critical to cultivate user awareness of potential risks and benefits to online privacy and self-disclosure that can help them evaluate rewards and drawbacks of online participation and make informed decisions. Technology designers may consider ways to establish trust with users, particularly marginalized individuals, perhaps through privacy heuristics (e.g., transparency) that explicitly inform users how their personal information is collected and handled. Although we do not advocate that participating in online activities is necessarily and equally beneficial for everyone, creating a trustworthy environment for marginalized groups, who tend to be less trusting compared to non-marginalized groups, could at least eliminate psychological barriers for them to feel empowered when they go online.

Limitations and Future Research

Like all research, the findings of this study must be interpreted in light of the limitations of the research methods employed. This study conceptualizes marginalization based on dichotomous categories of education (with vs. without a college degree) and race (Whites and Asians vs. African Americans). Although circumstantial evidence for privacy divides as a result of these educational and racial differences has been well-documented (e.g., Auxier et al., 2019; Büchi et al., 2016), the dichotomy may have inevitably obscured nuances that could have occurred within each subgroup or across different pairings of subgroups (e.g., Asian vs. Latinos). These should be further disentangled, perhaps by collecting larger

samples across different sociodemographic groups of interest. Other traditional markers of marginalization, such as income, should also be taken into consideration.

One primary goal of this research was to test trust as an alternative explanation to digital skills that could be helpful for understanding differences in privacy attitudes and behavior. Thus privacy skills were not directly tested in this study. It is imperative for future research to investigate if trust and digital privacy skills may both serve as explanatory and/or conditional factors of the online privacy divide, and if so, under what circumstances each operates. This will require the development and validation of digital privacy skills scales suitable for different online contexts (e.g., Internet vs. social media). Moreover, purposive sampling was utilized to achieve the comparative goals of this research, but representative sampling is needed for future research to produce generalizable results in terms of understanding similarities and differences in marginalized and non-marginalized groups privacy attitudes and behavior in the population.

While this study takes a first step testing divides in privacy concerns and privacy management behaviors, it leaves untested whether privacy concerns predict privacy management behaviors on both the horizontal and vertical dimensions. Further research should fill in this gap, perhaps by leveraging the extended model of the privacy calculus (Dienlin & Metzger, 2016), to uncover whether the predictive power of privacy concerns, perceived benefits, and privacy self-efficacy on privacy management behaviors may be contingent upon education, race, and/or other markers of marginalization (e.g., perceived marginalization, income). In addition, potential divides in prominent psychological factors that impact privacy decisions, such as privacy self-efficacy and privacy cynicism, should be

incorporated into future investigations to further elaborate the boundary conditions of the online privacy divide construct.

Future research should also test the individualistic, networked, and institutional approaches proposed in the integrated model of online privacy (Bazarova & Masur, 2020), for example, by studying the dynamic processes through which marginalized individuals manage privacy and self-disclosure across these levels and their repercussions. One instance is algorithmic profiling, which may result from self-disclosure and information sharing at all three levels. As an example, employment decisions can be made by biased algorithmic processing of people's social media data, including network analysis of a potential employee's connections to measure their social capital within a certain field, and content analysis of social media posts to determine personality types (Madden et al., 2017). When such information is used as primary indicators of candidates' career success and propensity for relationship building, those with low income, disability, African Americans and Latinos are inevitably discriminated against in job opportunities, which may further exacerbate existing inequalities (McDonald & Forte, 2022). This example highlights the high stakes for online privacy divides in the real world, and underscores the need for further scholarly inquiry on this topic.

References

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding.* Brooks/Cole Publishing Company.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Baik, J., & Jang, E. (2022). Where horizontal and vertical surveillances meet: Sense-making of US COVID-19 contact-tracing apps during a health crisis. *Mobile Media & Communication*, 20501579221078674.

Bastick, Z., & Mallet-Garcia, M. (2022). Double lockdown: The effects of digital exclusion on undocumented immigrants during the COVID-19 pandemic. *New media & society*, *24*(2), 365-383.

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology*, *36*, 118-123.

Best, A. L., Fletcher, F. E., Kadono, M., & Warren, R. C. (2021). Institutional distrust among African Americans and building trustworthiness in the COVID-19 response: implications for ethical public health practice. *Journal of Health Care for the Poor and Underserved*, *32*(1), 90.

Betts, M. (2020). *African Americans' perceptions of racial inequality in relation to institutional and social trust* [Unpublished doctoral dissertation]. The University of Wisconsin-Milwaukee.

Brehm, J., & Rahn, W. (1997). Individual-level evidence for the causes and consequences of social capital. *American Journal of Political Science*, *41*, 999-1023.

Bronfenbrenner U (1979) *The ecology of human development*. Cambridge, MA: Harvard University Press.

Büchi, M., Festic, N., Just, N., & Latzer, M. (2021). Digital inequalities in online privacy protection: Effects of age, education and gender. In *Handbook of digital inequality* (pp. 296-310). Edward Elgar Publishing.

Büchi, M., Just, N., & Latzer, M. (2016). Modeling the second-level digital divide: A five-country study of social differences in Internet use. *New media & society*, *18*(11), 2703-2722.

Chen, W., & Li, X. (2022). Digital inequalities in American disadvantaged urban communities: Access, skills, and expectations for digital inclusion programs. *Information, Communication & Society*, *25*(13), 1916-1933.

Cohn, D., Brown, A., & Keeter, S. (2020, February 20). *Most adults aware of 2020 census and ready to respond, but don't know key details*. Pew Research Center. https://www.pewresearch.org/social-trends/2020/02/20/the-u-s-census-and-privacy-concerns/

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication*, *21*(5), 368-383.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinesen, P. T. (2012). Does generalized (dis) trust travel? Examining the impact of cultural heritage and destination-country environment on trust of immigrants. *Political Psychology, 33*(4), 495-511.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214-233.

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, *21*(5), 712-728.

Douds, K., & Wu, J. (2018). Trust in the bayou city: Do racial segregation and discrimination matter for generalized trust?. *Sociology of Race and Ethnicity*, *4*(4), 567-584.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook 'friends': Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–68.

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media+ Society*, *6*(2), 2056305120916853.

Evangelist, M. (2022). Narrowing Racial Differences in Trust: How Discrimination Shapes Trust in a Racialized Society. *Social Problems*, *69*(4), 1109-1136.

Gonzales, A. L., McLeod, C., Ince, J., Bell, J., & Anderson, P. (2021). *Building New Bridges: Strategies for Social Network Diversification by Race and Income*. Paper

presented at the 2021 annual National Communication Association Conference. Seattle, WA.

Graham, R. S., & Smith, S. K. (2018). African American digital practices: Mobile E-Health and residential segregation. *Sociological Focus*, *51*(3), 186 199. https://doi.org/10.1080/00380237.2018.1382291

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.1080/08838151.2012.732140

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of interactive advertising*, *10*(2), 28-45.

Hui, J., King, J., Mcleod, C., & Gonzales, A. (2023). High risk, high reward: Social networking online in under-resourced communities. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1-12.

Israni, A., Ellison, N. B., & Dillahunt, T. R. (2021). 'A Library of People': Online resource-seeking in low-income communities. In *Proceedings of the ACM on Human-Computer Interaction, 5(CSCW1)*, 1-28.

Jamison, A. M., Quinn, S. C., & Freimuth, V. S. (2019). "You don't trust a government vaccine": Narratives of institutional trust and influenza vaccination among African American and white adults. *Social Science & Medicine*, *221*, 87-94.

Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, *25*(1), 1-24.

Kalmus, V., Bolin, G., & Figueiras, R. (2022). Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. *New Media & Society*, 14614448221134493.

Katz, V.S. & Gonzalez, C. (2016). Community variations in low-income Latino families' technology adoption and integration. *American Behavioral Scientist, 60*(1) 59-80. doi:10.1177/0002764215601712

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. I*dentity in the Information Society*, *2*(1), 39-63

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109-125.

Krosnick, J. A., & Fabrigar, L. R. (1997). Designing rating scales for effective measurement in surveys. In L. Lyberg, P. Biemer, M. Collins, E. de Leeuw, C. Dippo, N. Schwarz, & D. Trewin (Eds.), *Survey measurement and process quality* (pp. 141-164). New York: John Wiley.

Levi, M., & Stoker, L. (2000). Political trust and trustworthiness. *Annual Review of Political Science*, *3*(1), 475-507.

Li, X., & Chen, W. (2021). Core tech support networks and digital inequalities in American disadvantaged urban communities. *Journal of Computer-Mediated Communication*, *26*(2), 91-107.

Li, X., Chen, W., & Straubhaar, J. D. (2018). Privacy at the margins| concerns, skills, and activities: Multilayered privacy issues in disadvantaged urban communities. *International Journal of Communication*, *12*, 22.

Liu, J. H., Milojev, P., Gil de Zúñiga, H., & Zhang, R. J. (2018). The global trust inventory as a "proxy measure" for social capital: Measurement and impact in 11 democratic societies. *Journal of Cross-Cultural Psychology*, *49*(5), 789-810.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. doi:10.1111/j.1540-4560. 1977.tb01880.x

López, N., Vargas, E., Juarez, M., Cacari-Stone, L., & Bettez, S. (2018). What's your "street race"? Leveraging multidimensional measures of race and intersectionality for examining physical and mental health status among Latinxs. *Sociology of Race and Ethnicity*, *4*(1), 49-66:

Lundmark, S., Gilljam, M., & Dahlberg, S. (2016). Measuring generalized trust: An examination of question wording and the number of scale points. *Public Opinion Quarterly*, *80*(1), 26-43.

Lutz, C., & Hoffmann, C. P. (2021). Inequalities in online political participation: The role of privacy concerns. In *Handbook of digital inequality* (pp. 326-340). Edward Elgar Publishing.

Madden, M. (2017, September 27). *Privacy, security, and digital inequality.* Data & Society Research Institute. https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*(1), 53-125.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Männiste, M., & Masso, A. (2018). The role of institutional trust in Estonians' privacy concerns. *Studies of Transition States and Societies, 10*(2).

Marwick, A., Fontaine, C., & Boyd, D. (2017). "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media+ Society, 3*(2), 2056305117710455.

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

Masur, P. K. (2021). Understanding the effects of conceptual and analytical choices on 'finding'the privacy paradox: A specification curve analysis of large-scale survey data. *Information, Communication & Society*, 1-19.

Masur, P. K., & Trepte, S. (2021). Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure. *Human Communication Research, 47*(1), 49-74.

McDonald, N., & Forte, A. (2022). Privacy and vulnerable populations. In *Modern socio-technical perspectives on privacy* (pp. 337-363). Springer, Cham.

Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in human behavior*, *28*(4), 1471-1477.

Metzger, M. J., & Suh, J. J. (2017). Comparative optimism about privacy risks on Facebook. *Journal of Communication, 67*(2), 203-232.

Min, S. J. (2019). From algorithmic disengagement to algorithmic activism: Charting social media users' responses to news filtering algorithms. *Telematics and Informatics, 43*, 101251. https://doi.org/10.1016/j.tele.2019.101251

Nabi, R. L., Prestin, A., & So, J. (2013). Facebook friends with (health) benefits? Exploring social network site use and perceptions of social support, stress, and well-being. *Cyberpsychology, Behavior, and Social Networking*, *16*(10), 721-727.

Pager, D., & Shepherd, H. (2008). The sociology of discrimination: Racial discrimination in employment, housing, credit, and consumer markets. *Annual Review of Sociology, 34*, 181-209.

Park, Y. J. (2021). Why privacy matters to digital inequality. In *Handbook of digital inequality* (pp. 284-295). Edward Elgar Publishing.

Pearce, K. E., & Rice, R. E. (2017). Somewhat separate and unequal: Digital divides, social networking sites, and capital-enhancing activities. *Social Media+ Society, 3*(2), 2056305117716272.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Redmiles, E. M., & Buntain, C. L. (2021). How feelings of trust, concern, and control of personal online data influence web use. In *Handbook of digital inequality* (pp. 311-325). Edward Elgar Publishing.

Rainie, L., Keeter, S., & Perrin, A. (2019). *Trust and distrust in America*. Pew Research Center. https://www.pewresearch.org/politics/2019/07/22/trust-and-distrust-in-america/

Rice, R. E. & Hoffman, Z. T. (2018). Attention in business press to the diffusion of attention technologies, 1990-2017. *International Journal of Communication, 12*. https://ijoc.org/index.php/ijoc/article/view/8250/2424

Richardson, A., Allen, J. A., Xiao, H., & Vallone, D. (2012). Effects of race/ethnicity and socioeconomic status on health information-seeking, confidence, and trust. *Journal of Health Care for the Poor and Underserved*, *23*(4), 1477-1493.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114.

Rosenberg, M. (1956). Misanthropy and political ideology. *American Sociological Review*, *21*(6), 690-695

Sannon, S., & Forte, A. (2022). Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next. In *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1-33.

Shrider, E. A., Kollar, M., Chen, F., & Semega, J. (2021). Income and poverty in the United States: 2020. *Current Population Reports. US Census Bureau*. https://www.census.gov/library/publications/2021/demo/p60-273.html

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15-22.

Smith, S. S. (2010). Race and trust. *Annual Review of Sociology*, *36*, 453-475.

Sønderskov, K. M., & Dinesen, P. T. (2016). Trusting the state, trusting each other? The effect of institutional trust on social trust. *Political Behavior*, *38*(1), 179-202.

Taylor, P., Funk, C., & Clark, A. (2007, February 22). *Americans and social trust: who, where and why*. Pew Research Center. https://www.pewresearch.org/social-trends/2007/02/22/americans-and-social-trust-who-where-and-why/

Twenge, J. M., Campbell, W. K., & Carter, N. T. (2014). Declines in trust in others and confidence in institutions among American adults and late adolescents, 1972–2012. *Psychological Science*, *25*(10), 1914-1923.

U.S. Census Bureau. (2022, February). *Census bureau releases new educational attainment data*. https://www.census.gov/newsroom/press-releases/2022/educational-attainment.html

van Deursen, A. J. A. M., & van Dijk, J. A. (2012). *Trendrapport internetgebruik 2012: een Nederlands en Europees perspectief*. Enschede: University of Twente.

van Dijk, J. (2020). *The digital divide*. John Wiley & Sons.

van Ooijen, I., Segijn, C. M., & Opree, S. J. (2022). Privacy Cynicism and its Role in Privacy Decision-Making. *Communication Research*, 00936502211060984.

Vitak, J., Liao, Y., Subramaniam, M., & Kumar, P. (2018). 'I Knew It Was Too Good to Be True" The challenges economically disadvantaged internet users face in assessing trustworthiness, avoiding scams, and developing self-efficacy online. In *Proceedings of the ACM on human-computer interaction, 2(CSCW)*, 1-25.

Walker, A. M., & Hargittai, E. (2021). Drills and spills: Developing skills to protect ones privacy online. In *Handbook of digital inequality* (pp. 358-372). Edward Elgar Publishing.

Wang, L. H., & Metzger, M. J. (2021). The role of culture in privacy management on social media among emerging adult children and their parents. *Journal of International and Intercultural Communication*, 1-29.

Williamson, L. D. (2021). Beyond personal experiences: Examining mediated vicarious experiences as an antecedent of medical mistrust. *Health Communication*, *37*(9), 1061-1074.

Wilkes, R., & Wu, C. (2019). Immigration, discrimination, and trust: A simply complex relationship. *Frontiers in Sociology*, *4*, 32.

Zmerli, S., & Newton, K. (2008). Social trust and attitudes toward democracy. *Public Opinion Quarterly*, *72*(4), 706-724.

Appendix A: Tables

Table 1
Sample Demographics

Sample demographics	n	%
Education		
Less than high school degree	32	2.3%
High school graduate (high school diploma or equivalent including GED)	330	23.6%
Some college but no degree	329	23.5%
Associate degree in college (2-year)	198	14.1%
Bachelor's degree in college (4-year)	365	26.1%
Master's degree	111	7.9%
Doctoral degree	16	1.1%
Professional degree (JD, MD)	20	1.4%
Race/Ethnicity		
Hispanic, Latina/Latino, Latine, or Latinx	280	20%
White	360	25.7%
Black, African, or African American	354	25.3%
East Asian	215	15.3%
South East Asian	59	4.2%
South Asian	47	3.4%
Native Hawaiian or Other Pacific Islander	16	1.1%
Native American, American Indian, or Alaskan Native	2	.1%
Middle Eastern or North African	4	.3%
Mixed races	61	4.4%
I prefer to self-describe	3	.2%

Table 2
Summary of Results

Hypotheses/Research Questions	Results	Supported?
H1: People without a college degree will report higher (a) horizontal and (b) vertical privacy concerns on social media than those with a college degree.	People without a college degree reported *lower* (a) horizontal and (b) vertical privacy concerns than those with a college degree.	Not supported.
H2: African Americans and Latinos will report higher (a) horizontal and (b) vertical privacy concerns on social media than Whites and Asians.	No main effects for race on (a) horizontal and (b) vertical privacy concerns.	Not supported.
H3: Education and race will interact to impact privacy concerns such that African Americans and Latinos who do not have a college degree will report the highest (a) horizontal and (b) vertical privacy concerns on social media among all educational and racial groups.	No significant interaction effect of education and race on privacy concerns.	Not supported.
RQ1: Does education impact the frequency of using (a) horizontal and (b) vertical privacy management strategies on social media?	No main effects for education on the frequency of using (a) horizontal and (b) vertical privacy management strategies.	N/A
RQ2: Does race impact the frequency of using (a) horizontal and (b) vertical privacy management strategies on social media?	African Americans and Latinos reported using both (a) horizontal and (b) vertical strategies more frequently.	N/A
RQ3: Do education and race interact to impact the frequency of using (a) horizontal and (b) vertical privacy management strategies on social media?	No significant interaction effects on the use of privacy management strategies.	N/A
H4: Generalized social trust will mediate the impacts of education and race on horizontal privacy concerns on social media, such that (a) people without a college degree and (b) African Americans and Latinos will report lower social trust, which will predict higher horizontal concerns, compared to people with a college degree and Whites and Asians.	Generalized social trust partially mediated the impact of education on horizontal concerns, but did not mediate the impact of race.	Partially supported.

H5: Generalized social trust will mediate the impacts of education and race on the frequency of using horizontal privacy management strategies, such that (a) people without a college degree and (b) African Americans and Latinos will report lower generalized social trust, which will predict higher frequency of using horizontal strategies, compared to people with a college degree and Whites and Asians.	Generalized social trust mediated the impacts of education, but not race on horizontal strategies use.	Partially supported.
H6: Institutional trust will mediate the impacts of (a) education and (b) race on vertical privacy concerns, such that (a) people without a college degree and (b) African Americans and Latinos will report lower generalize social trust, which will predict higher vertical concerns.	Institutional trust mediated the impact of education and race on vertical privacy concerns.	Supported.
H7: Institutional trust will mediate the relationship between (a) education, (b) race and the frequency of using vertical privacy management strategies, such that (a) people without a college degree and (b) African Americans and Latinos will report higher frequency of using vertical strategies indirectly through institutional trust.	Institutional trust mediated the impact of race on the use of vertical privacy management strategies (though in the opposite directionality than predicted), but did not mediate the impact of education.	Not supported

Appendix B: Measures

Horizontal Privacy Concerns (*M* = 4.46, *SD* = 1.15)

Think about friends, family members, coworkers, employers, strangers, and other individual social media users that may have access to your personal information on social media, please indicate how much you agree or disagree with the following statements:

1-7: [Strongly disagree; Disagree; Somewhat disagree; Neither agree nor disagree; Somewhat agree; Agree; Strongly agree]

1. I am concerned that someone I don't expect (e.g., a stranger, my "ex", my parents, teacher, boss) could view my social media profile (*M* = 4.37, *SD* = 1.82).
2. I am concerned that I cannot limit access to some information I publish on social media for some people (*M* = 4.53, *SD* = 1.70).
3. I feel uncomfortable that people who I don't know might follow changes in my social media (*M* = 4.51, *SD* = 1.73).
4. If I was in a job application process, I would make many changes to my profile (*M* = 3.78, *SD* = 1.84).
5. I don't care what opinion others build about me based on what I post on social media (*M* = 4.59, *SD* 1.75).
6. I am concerned that I don't have control over what other users do with information I post on social media (*M* = 4.75, *SD* = 1.65).
7. It sometimes bothers me that other users can tag me or post something about me on their social media (*M* = 4.52, *SD* = 1.71).
8. I am concerned that other users might take advantage of the information they learn about me through social media (*M* = 4.83, *SD* = 1.62).
9. It worries me that other users could use the information they have collected about me from social media for identity theft (*M* = 5.01, *SD* = 1.67).
10. I am concerned that other users could use the information they have collected about me from social media for financial scams (*M* = 4.84, *SD* = 1.70).

Vertical Privacy Concerns (*M* = 4.66, *SD* = 1.23)

Think about government agencies, social media companies, advertisers, corporations, and other organizations that may have access to your personal information on social media, please indicate how much you agree or disagree with the following statements:

1-7: [Strongly disagree; Disagree; Somewhat disagree; Neither agree nor disagree; Somewhat agree; Agree; Strongly agree]

1. It never actually worries me that social media companies (e.g., Facebook, Instagram) collect and store information about me over the years (*M* = 3.64, *SD* = 1.84).
2. I am concerned that social media companies (e.g., Facebook, Instagram) could share the information I provide with other parties (e.g., marketing, government agencies) (*M* = 5.05, *SD* = 1.59).
3. It worries me that other parties (e.g., marketers, government or law enforcement agencies) could use the information they have collected about me from social media for commercial or surveillance purposes (*M* = 4.84, *SD* = 1.66).
4. It bothers me that the information in my social media profile may be used to display personalized advertising to me (*M* = 4.77, *SD* = 1.64).

5. I am concerned that the power the government and law enforcement have to wiretap my social media activities might threaten the safety of me and my family (*M* = 4.52, *SD* = 1.76).
6. I am concerned that my social media information (e.g., e-mails, shopping records, online surfing history, interest groups joined, etc.) gathered by the government and law enforcement might be used against me in a court of law (*M* = 4.47, *SD* = 1.78).
7. I am concerned that my legal rights might be threatened as a result of the government and law enforcement's ability to monitor social media activities (*M* = 4.62, *SD* = 1.74).

Horizontal Privacy Management Strategies (*M* = 2.41, *SD* = .97)

Now, think about friends, family members, coworkers, employers, strangers, and other individual users on social media that may have access to your personal information on social media. How often have you used the following strategies to protect your privacy from these social media users?

1-5: [Never; Rarely; Sometimes; Often; Always]

1. Intentionally limit the breadth and/or depth of what I post on social media (*M* = 2.73, *SD* = 1.40).
2. Use an exclusive disclosure list to limit my posts to certain contacts (*M* = 2.34, *SD* = 1.35).
3. Block certain contacts from seeing a post by or about me (*M* = 2.64, *SD* = 1.29).
4. Review, delete, or untag posts made by others about me (*M* = 2.49, *SD* = 1.31).
5. Use private messaging so people on social media won't see the content (*M* = 2.92, *SD* = 1.34).
6. Have a fake account (e.g., "finstagram") (*M* = 1.87, *SD* = 1.22).
7. Set posts to be invisible after a period of time (e.g., 24 h, 3 days) (*M* = 2.13, *SD* = 1.31).
8. Use shorthand, codewords, fake names, or slang language (*M* = 2.19, *SD* = 1.28).

Vertical Privacy Management Strategies (*M* = 2.46, *SD* = .97)

Now, think about government agencies, social media companies, advertisers, corporations, and other organizations that may have access to your personal information on social media. How often have you used the following strategies to protect your privacy from these entities?

1-5: [Never; Rarely; Sometimes; Often; Always]

1. Change the privacy settings or ad preferences to stop social media companies from tracking my personal information for commercial or surveillance purposes (*M* = 2.67, *SD* = 1.33).
2. Attempt to control or manipulate social media algorithms so that they cannot accurately track my information or preferences (*M* = 1.97, *SD* = 1.28).
3. Not link personal information, such as phone numbers or email addresses, across social media accounts (*M* = 2.84, *SD* = 1.41).
4. Use fake names or provide inaccurate information about myself on social media so that I cannot be tracked by government agencies, social media companies, and other organizations that might collect my data (*M* = 2.06, *SD* = 1.29).
5. Avoid posting information that may be seen as problematic by government agencies or law enforcement if they monitor my social media accounts (*M* = 2.75, *SD* = 1.46).

6. Not use, or entirely leave social media because they ask for too much personal information (*M* = 2.36, *SD* = 1.29).
7. Review privacy policies of social media to learn how they handle my data (*M* = 2.55, *SD* = 1.30).

Generalized Social Trust (*M* = 3.60, *SD* = .97)
Please indicate how much you agree with the following statements:
1-7: [Strongly disagree; Disagree; Somewhat disagree; Neither agree nor disagree; Somewhat agree; Agree; Strongly agree]

1. Generally speaking, most people can be trusted (*M* = 3.96, *SD* = 1.65).
2. Generally speaking, you need to be very careful in dealing with people (*M* = 5.47, *SD* = 1.30).
3. Most people try to be fair (*M* = 4.47, *SD* = 1.39).
4. Most people would try to take advantage of you if they got the chance (*M* = 3.18, *SD* = 1.47).
5. Most of the time people try to be helpful (*M* = 4.68, *SD* = 1.35).
6. Most of the time people are mostly looking out for themselves (*M* = 5.24, *SD* = 1.32).

Institutional Trust (*M* = 4.20, *SD* = 1.19)
How much do you trust the following institutions and organizations?
1-7: [Do not trust at all; Mostly do not trust; Somewhat do not trust; Neither distrust nor trust; Somewhat trust; Mostly trust; Trust completely]

1. The US judicial (court) system (*M* = 4.01, *SD* = 1.70)
2. The executive branch of the federal government (e.g., the President and the President's cabinet) (*M* = 3.91, *SD* = 1.72)
3. The US Congress (*M* = 3.71, *SD* = 1.67)
4. The US military (*M* = 4.58, *SD* = 1.66)
5. Police and other law enforcement agencies (*M* = 4.11, *SD* = 1.75)
6. Scientists (*M* = 4.98, *SD* 1.42)
7. Medical and healthcare system (doctors, health insurers, etc.) (*M* = 4.86, *SD* = 1.55)
8. Banks and financial institutions (*M* = 4.41, *SD* = 1.58)
9. Large corporations (*M* = 3.66, *SD* = 1.62)
10. Religious organizations (*M* = 4.07, *SD* = 1.77)
11. Educators (*M* = 4.89, *SD* = 1.41)
12. News and entertainment media companies (*M* = 3.80, *SD* = 1.64)
13. Social media companies (*M* = 3.55, *SD* = 1.63)

Previous Privacy Violation Experiences on Social Media (*M* = 1.54, *SD* = .50)
Have you or people close to you ever had a negative privacy experience (e.g., been a victim of an online scam, had personal information stolen, persistent and unwanted contact from someone online) on social media?
[Yes= 1; No= 0]

Race/Ethnicity
What's your race or ethnicity (i.e., your heritage, ancestry, or origin)? (select all that apply)

1. Hispanic, Latina/Latino, Latine, or Latinx (e.g., Mexican, Chicano/Chicana, Guatemalan, or Honduran ancestry)
2. White (e.g., Caucasian, Anglo, or European ancestry)
3. Black, African, or African American
4. East Asian (e.g., Chinese, Japanese, or Korean ancestry)
5. South East Asian (e.g., Cambodian, Laotian, or Vietnamese ancestry)
6. South Asian (e.g., Indian or Pakistani ancestry)
7. Native Hawaiian or Other Pacific Islander (e.g., Filipino, Samoan, or Tongan ancestry)
8. Native American, American Indian, or Alaskan Native
9. Middle Eastern or North African (e.g., Egyptian, Algerian, Iranian, Lebanese, Moroccan, or Palestinian ancestry)
10. I prefer to self-describe: _____

Education

What is the highest level of school you have completed or the highest degree you have received?

1. Less than high school degree
2. High school graduate (high school diploma or equivalent including GED)
3. Some college but no degree
4. Associate degree in college (2-year)
5. Bachelor's degree in college (4-year)
6. Master's degree
7. Doctoral degree
8. Professional degree (JD, MD)

Income

Information about income is very important to understand. Would you please give your best guess? Please indicate the answer that includes your entire household income in (previous year) before taxes.

1. Under $5,000
2. $5,000 to $9,999
3. $10,000 to $14,999
4. $15,000 to $19,999
5. $20,000 to $24,999
6. $25,000 to $29,999
7. $30,000 to $34,999
8. $35,000 to $39,999
9. $40,000 to $44,999
10. $45,000 to $49,999
11. $50,000 to $54,999
12. $55,000 to $59,999
13. $60,000 to $64,999
14. $65,000 to $69,999
15. $70,000 to $74,999
16. $75,000 to $79,999

17. $80,000 to $84,999
18. $85,000 to $89,999
19. $90,000 to $94,999
20. $95,000 to $99,999
21. $100,000 to $104,999
22. $105,000 to $109,999
23. $110,000 to $114,999
24. $115,000 to $119,999
25. $120,000 to $124,999
26. $125,000 to $129,999
27. $130,000 to $134,999
28. $135,000 to $139,999
29. $140,000 to $144,999
30. $145,000 to $149,999
31. $150,000 to $154,999
32. $155,000 to $159,999
33. $160,000 to $164,999
34. $165,000 to $169,999
35. $170,000 to $174,999
36. $175,000 to $179,999
37. $180,000 to $184,999
38. $185,000 to $189,999
39. $190,000 to $194,999
40. $195,000 to $199,999
41. $200,000 and over

Sex/Gender Identity

What is your gender identity?

1. Female
2. Male
3. Non-binary
4. I prefer to self-describe: _____

Age

What is your age (in years old)? _____

Frequency of Social Media Posting (*M* = 3.66, *SD* = 1.99)

On average, how often do you add new content to your social media account (e.g., posts, stories, etc.)

1-8: [Never; Less than once a month; About one or twice a month; About once a week; A few times a way; About once every few days; About one or twice a day; Several times a day]

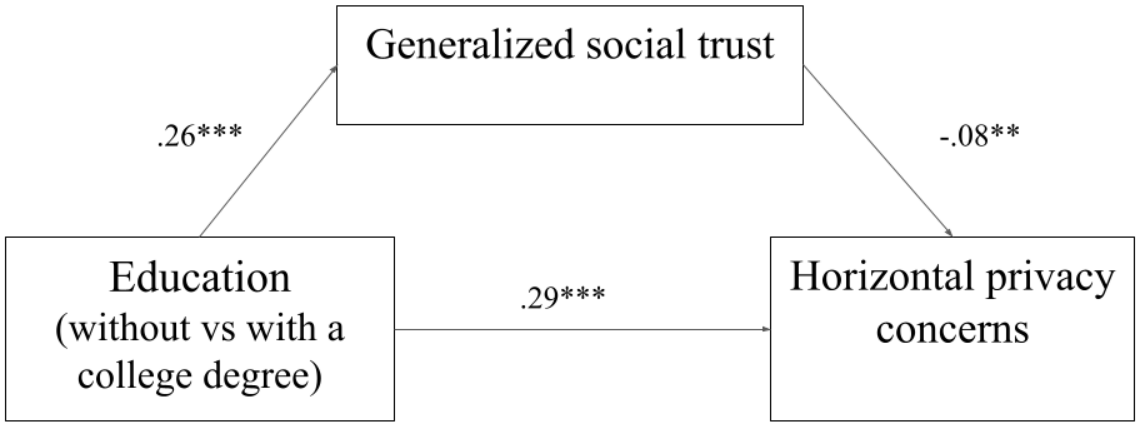
1. Never
2. Less than once a month
3. About once or twice a month
4. About once a week
5. A few times a week

6. About once every few days
7. About once or twice a day
8. Several times a day

Appendix C: Figures

Figure 1

Generalized Social Trust as a Mediator of the Relationship Between Education and Horizontal Privacy Concerns (H4a)

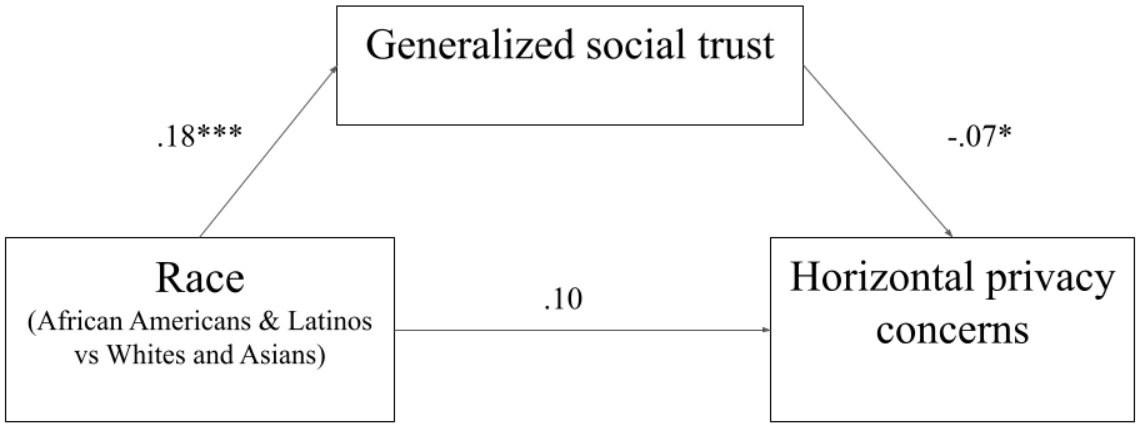


Notes. Indirect effect = -.02, CI[-.04, -.00], with 5000 sample bootstraps.

*p < .05, **p < .01, ***p < .001

Figure 2

Generalized Social Trust as a Mediator of the Relationship Between Race and Horizontal Privacy Concerns (H4b)

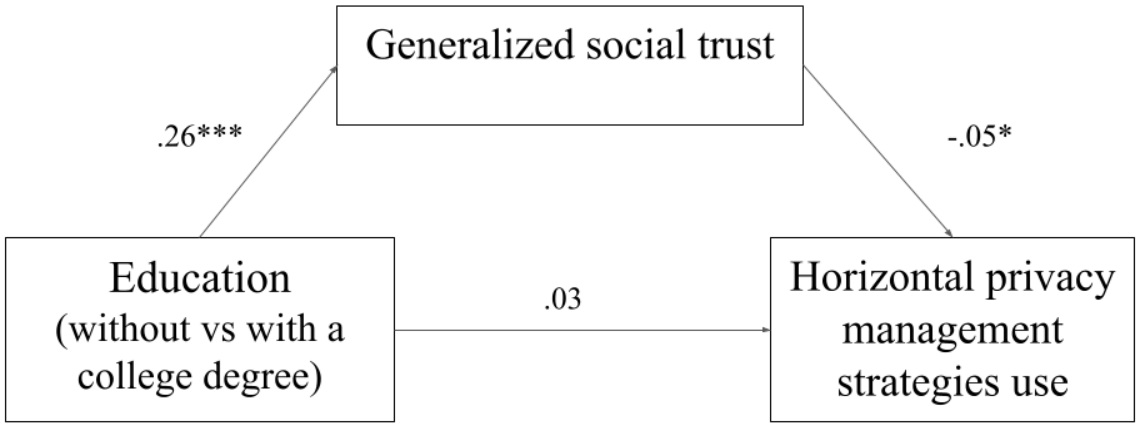


Notes. Indirect effect = -.01, CI[-.03, .00], with 5000 sample bootstraps.

*$p < .05$, **$p < .01$, ***$p < .001$

Figure 3

Generalized Social Trust as a Mediator of the Relationship Between Education and Horizontal Privacy Management Strategies Use (H5a)

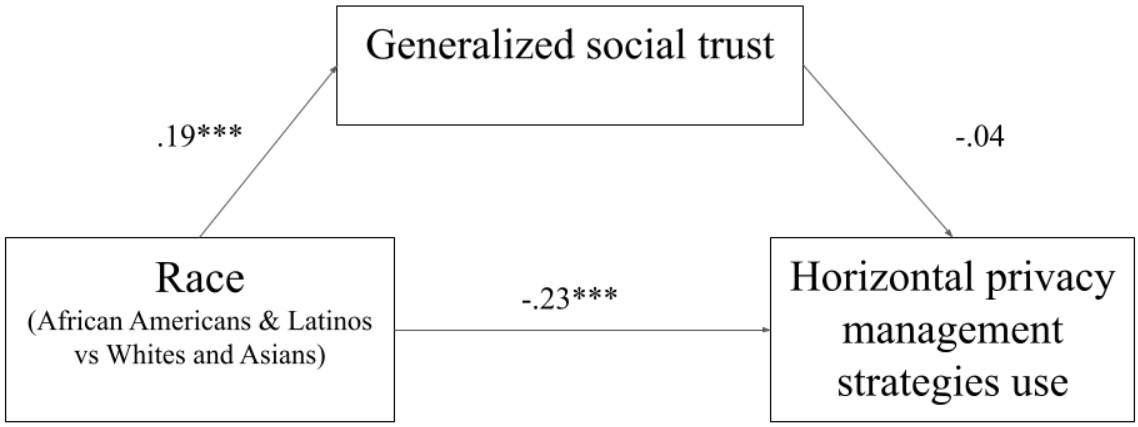


Notes. Indirect effect = -.01, CI[-.03, -.00], with 5000 sample bootstraps.

*$p < .05$, **$p < .01$, ***$p < .001$

Figure 4

Generalized Social Trust as a Mediator of the Relationship Between Race and Horizontal Privacy Management Strategies Use (H5b)

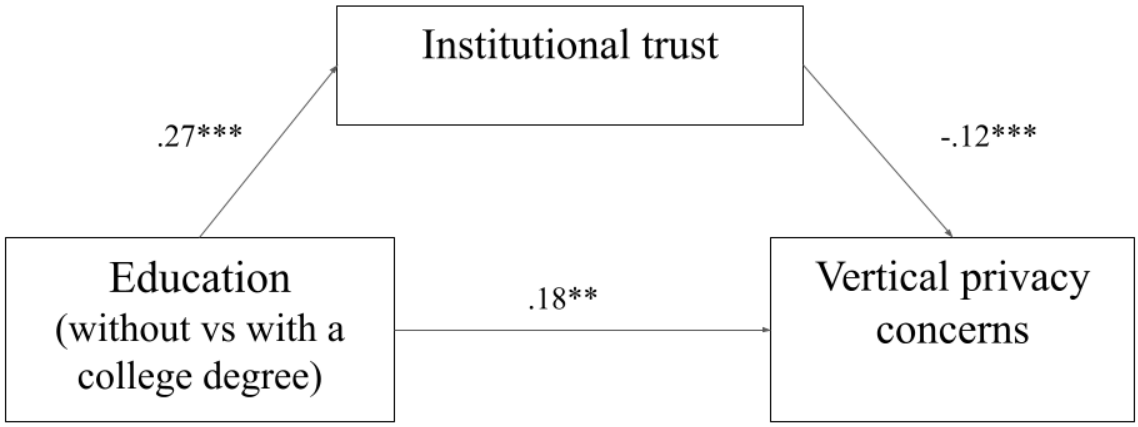


Notes. Indirect effect = -.01, CI[-.02, .00], with 5000 sample bootstraps.

*$p < .05$, **$p < .01$, ***$p < .001$

Figure 5

Institutional Trust as a Mediator of the Relationship Between Education and Vertical Privacy Concerns (H6a)

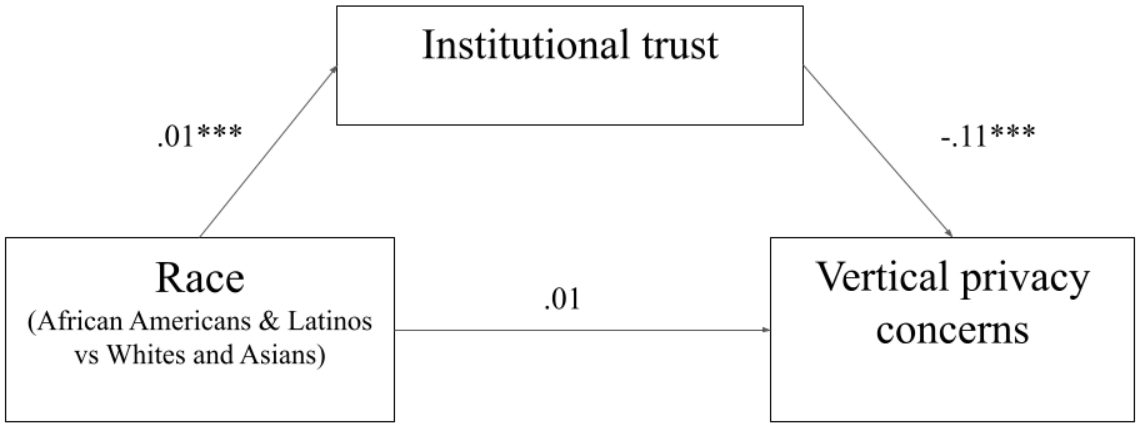


Notes. Indirect effect = -.03, CI[-.06, -.01], with 5000 sample bootstraps.

*$p < .05$, **$p < .01$, ***$p < .001$

Figure 6

Institutional Trust as a Mediator of the Relationship Between Race and Vertical Privacy Concerns (H6b)

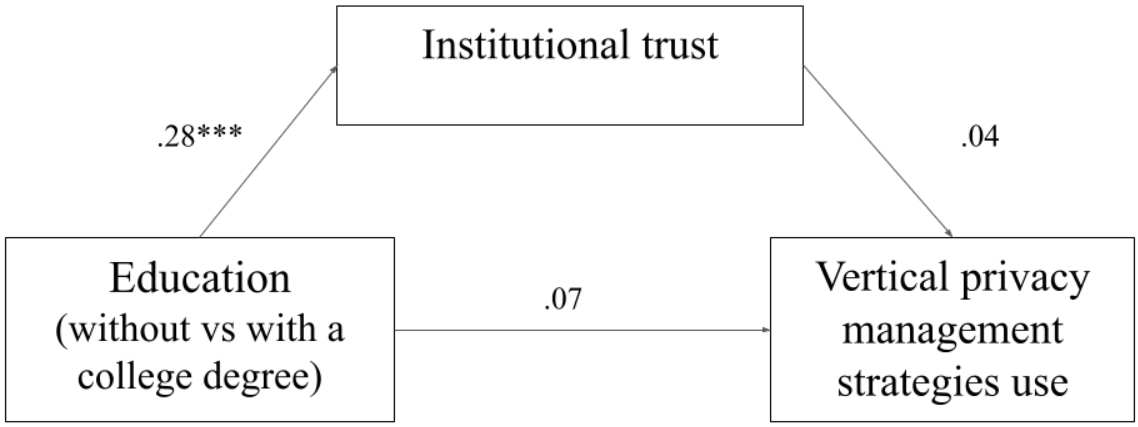


Notes. Indirect effect = -.02, CI[-.04, -.01], with 5000 sample bootstraps.

*$p < .05$, **$p < .01$, ***$p < .001$

Figure 7

Institutional Trust as a Mediator of the Relationship Between Education and Vertical Privacy Management Strategies Use (H7a)

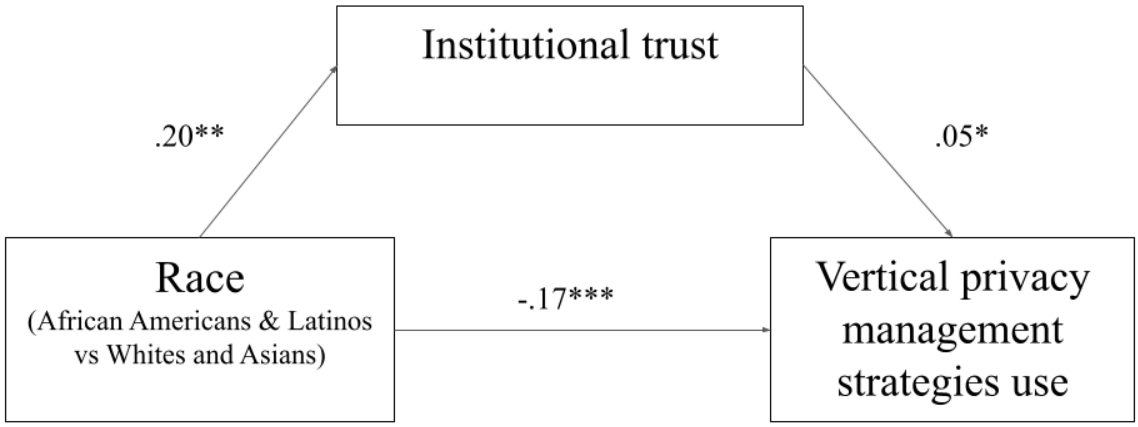


Notes. Indirect effect = .01, CI[-.00, .03], with 5000 sample bootstraps.

*$p < .05$, **$p < .01$, ***$p < .001$

Figure 8

Institutional Trust as a Mediator of the Relationship Between Race and Vertical Privacy Management Strategies Use (H7b)



Notes. Indirect effect = .01, CI[.00, .02], with 5000 sample bootstraps.

*$p < .05$, **$p < .01$, ***$p < .001$