The State of Consumer Safety Perceptions and Brand Loyalty in the Data Privacy Crisis

Rebecca Townsend Scott
Le Moyne College

Magdoleen Ierlan
Le Moyne College

Data privacy and sharing with third parties continue to be prominent societal issues that have consumers questioning the safety of their personal information. In addition, significant global events are proposed as having an impact on consumer perceptions of safety. Using the Online Privacy Concern Scale and the Neuroception of Psychological Safety Scale informed by Polyvagal Theory, this research examines reactions to specific types of data sharing and how feelings of safety impact privacy concerns. The research also looks to understand how feelings of safety toward a brand impact consumer loyalty. Being the first study that applies these two scales, this research offers several important implications regarding data privacy and consumer safety perceptions.

Keywords: data privacy, data sharing, privacy protections, privacy thresholds, safety perceptions, brand loyalty

INTRODUCTION

With the increased monetization of personal data, the topic of data privacy has become globally prevalent for consumers, companies, and governments. Society is facing an online data and privacy crisis (Segal, 2022), and despite highly publicized data breaches (Klosowski, 2021), increases in identity theft incidents (Insurance Information Institute, 2022), and data privacy protections being implemented overseas (Klosowski, 2021), comprehensive data privacy laws have not been enacted in the United States (Singer, 2019). Recent research confirms that consumers are concerned about data privacy (Pew Research Center, 2019); however, these concerns vary based on the data collected, personal thresholds, and other factors (PwC, 2022). Moreover, despite these concerns, most consumers are not actively pursuing accessible data privacy protections (Anant et al., 2020). This study aims to understand consumer data privacy sentiments in the present environment and uncover further insights into these nuances.

Consumer data privacy research is extensive; however, examining how recent global events have influenced this topic warrants deeper exploration. The global COVID-19 pandemic and other significant world events have compromised consumers' sense of safety (Morton, 2022), raising questions about how these changes have affected consumer perceptions of safety in the context of data privacy. Specifically, how does the perception of data safety influence consumer sentiments and behaviors toward the companies and brands collecting their data? Furthermore, what types of personal data sharing are deemed unacceptable,

what actions will consumers take against brands in response to data privacy violations, and how confident are they in pursuing those actions? These are the questions this research seeks to address.

Although online privacy concerns, safety perceptions, and brand loyalty have been studied separately, their intersection in the current landscape remains unexplored. This study is the first to combine the Neuroception of Psychological Safety Scale and the Online Privacy Concern Scale to examine the potential relationship between consumer safety perceptions and online privacy concerns. Additionally, this study enhances the understanding of privacy thresholds for specific types of personal information and investigates whether a relationship exists between consumer feelings of safety and brand loyalty. The findings will provide important theoretical insights into data privacy concerns, safety perceptions, brand loyalty, and privacy protection behaviors, offering potential actions for consumers and brands to effectively address current challenges.

LITERATURE REVIEW

Consumer Data Privacy Concerns

Data privacy concerns have been on the rise in the United States for decades. Ninety percent of consumers express concern about online privacy, and nearly 50% have limited online activity due to privacy concerns (Boudet et al., 2019). While several countries, including those in Europe, have implemented comprehensive consumer data privacy protections, the United States remains one of the few developed nations without formalized consumer data privacy laws or an independent agency to enforce them (Singer, 2019). As of this publication, no federal regulation exists, and only four states have successfully implemented consumer data privacy laws (NG, 2023). The implications of weak privacy protections range from minor inconveniences, such as unwanted digital ads and junk email, to severe consequences, including account hacking and identity theft. Twenty-eight percent of Americans report experiencing at least one of three major identity theft issues within the past 12 months: fraudulent charges on credit or debit cards (21%), unauthorized access to social media or email accounts (8%), and attempts to open credit lines or obtain loans in their name (6%) (Pew Research Center, 2019). The lack of regulatory action to address these concerns underscores the need to examine consumer sentiments toward data privacy. Three resounding themes—complacency, fatigue, and self-efficacy perceptions—appear to shape consumer viewpoints on this issue.

Consumer Complacency

Despite the growing data privacy crisis, consumers exhibit a sense of complacency. A study found that nearly six in ten U.S. adults believe it is impossible to go through daily life without having their data collected by companies (Pew Research Center, 2019). Furthermore, 82% of consumers are willing to share some type of personal data in exchange for a more personalized service experience (PwC, 2022). Personal identifiers, such as birthdate and age (48%), sex/gender identity (45%), and race/ethnicity (37%), as well as contact information, such as an email address (61%), mailing address (40%), and phone number (35%), are commonly shared (PwC, 2022). However, consumers are more hesitant to share data related to usage and biometrics, with only 22% willing to share product usage data, 15% willing to share their mobile phone location, 5% consenting to facial recognition, and 3% sharing fingerprint data (PwC, 2022). This suggests that while consumers accept data collection for services and convenience, there are clear boundaries regarding the data types they are willing to disclose. Additionally, studies indicate that the more users like an app, the less they engage in privacy protection behaviors (Wottrich et al., 2019). When users perceive an app's risk to outweigh its benefits, they are more likely to consider it insecure (Balapour et al., 2019). Interestingly, higher knowledge levels about data collection practices correlate with lower motivation to protect privacy, implying that consumers with greater awareness feel resigned to the difficulty of mitigating these risks (Wottrich et al., 2019). These findings illustrate how consumer experiences with brands, companies, and applications influence their acceptance of data acquisition and reluctance to engage in privacy-protection behaviors.

Consumer Fatigue and Powerlessness

Recent research identifies a sense of consumer fatigue and powerlessness regarding data privacy. One study suggests that users have limited cognitive capacity to process privacy issues and, upon reaching a certain threshold, their intention to protect their privacy declines significantly (Tian et al., 2022). Privacy fatigue has been shown to impact users' final disclosure intentions more than privacy concerns (Tian et al., 2022). In a Pew Research Center survey, 48% of Americans reported feeling they have no control over who can access their search terms, and 41% felt similarly about the websites they visit (Pew Research Center, 2019). This perceived lack of control is reflected in consumer engagement with privacy protection measures: 38% of adults say they sometimes read privacy policies, while 36% never read them before agreeing to terms (Pew Research Center, 2019). Only 27% of internet users employ ad blockers (Statista, 2021), 14% encrypt their online communications, and just one-third regularly change their passwords (Anant et al., 2020). These findings support the idea that the current data privacy landscape leaves many consumers powerless or too overwhelmed to take protective action.

Self-Efficacy and Confidence Perceptions

Consumers also display conflicted self-efficacy regarding data privacy. A survey found that 63% of Americans understand very little or nothing about existing data privacy laws and regulations (Pew Research Center, 2019). Mobile app users exhibit relatively low self-efficacy, with many feeling unsure of how to engage in protective behaviors or believing they cannot do so (Wottrich et al., 2019). At the same time, 59% of consumers believe that companies prioritize profiting from their data over protecting it, yet they tend to trust the companies they choose to do business with (Boehm et al., 2022). Indeed, 70% of consumers express at least moderate confidence that the companies from which they purchase products and services adequately protect their data (Boehm et al., 2022). These findings highlight the paradoxical nature of consumer attitudes—while individuals express concerns about corporate data practices, they simultaneously demonstrate trust in their preferred brands, reinforcing inaction and self-doubt.

The Intersection of Psychological Safety and Data Privacy

At this time, the United States continues to recover from the global COVID-19 pandemic. The pandemic's legacy has heightened stress, anxiety, and trauma among the general population (Morton, 2022). Alongside other significant global events—including economic recessions, rising living costs, job insecurity, climate change, political turbulence, and the war in Ukraine—these stressors contribute to widespread psychological threats (Morton, 2022). While the long-term consequences of these events remain unclear, this study aims to explore their short-term effects and how perceptions of safety in the face of psychological threats intersect with the ongoing data privacy crisis. Expanding on Masur's (2018) situational privacy theory, which examines how interpersonal, environmental, and situational factors influence privacy literacy and self-disclosure, this research also builds on Morton et al.'s (2022) findings regarding the role of psychological safety in shaping data privacy thresholds and consumer-brand relationships. The results will explain how consumer data privacy, safety perceptions, and brand loyalty interconnect.

Psychological safety is central to mental health, well-being, and recovery (Morton, 2022). However, few studies have explored the relationship between consumer safety perceptions and data privacy. Research suggests that smartphones provide users with comfort and security (Melumad & Pham, 2020), leading to greater disclosure on mobile devices than on personal computers (Tian et al., 2022). Meanwhile, 70% of adults believe their data is less secure than five years ago, and 79% express concern about how companies use their data (Pew Research Center, 2019). As privacy concerns rise, consumers are likelier to engage in protective behaviors (Wottrich et al., 2019). Nevertheless, consumers often trust companies with transparent data privacy policies, with 85% valuing such policies before purchasing (Boehm et al., 2022). Approximately 40% have withdrawn business from a company due to data misuse, and 71% would stop engaging with a brand if it shared sensitive data without permission (Anant et al., 2020).

Against this backdrop, this study aims to deepen the understanding of how psychological safety, data privacy concerns, and brand trust interact, contributing to the broader discourse on consumer behavior and data protection.

Hypothesis Development

Present psychological threats are affecting consumer safety perceptions (Morton, 2022), and when compounded with online privacy concerns, they influence protective behaviors. Because feelings of safety impact decision-making, we infer that consumers who do not feel safe or experience lower levels of psychological safety will have greater online privacy concerns. Thus, we propose the following hypothesis:

H1: *Consumers who do not feel safe will have higher online privacy concerns.*

Consumers value digital trust and demand data privacy transparency from the companies and brands they engage with (Boehm et al., 2022). We propose that consumer trust fosters brand loyalty, reducing privacy protection behaviors and raising the threshold for switching brands. Therefore, our second hypothesis is:

H2: *Brands that make consumers feel safe will experience higher loyalty, making consumers less likely to switch brands.*

Consumers have varying preferences and thresholds regarding the shareability of their personal information, including the types of data collected by brands (PwC, 2022). Research has shown that while consumers accept certain data collection practices for convenience or in exchange for services, they perceive some types of data as more private. Based on gaps in existing research, we identify personal photos, direct messages, current location, and product usage data as particularly sensitive. If consumers discover that a brand shares these data types with third parties, they are more likely to feel concerned and take steps to protect their privacy. Thus, our third hypothesis is:

H3: *If consumers discover that a brand shares personal photos, direct messages, current location, or product usage data with a third party, they will be more likely to switch brands.*

Against this backdrop, this study aims to deepen the understanding of how psychological safety, data privacy concerns, and brand trust interact, contributing to the broader discourse on consumer behavior and data protection.

METHODOLOGY

Building on insights from the literature, we developed an online questionnaire grounded in established research methodologies. The survey incorporated validated measurement scales, a reputable survey platform, and a broad online dissemination strategy. Items were adapted to align with this study's focus on consumer data privacy, safety perceptions, and brand loyalty.

Sample and Data Collection

The target population included U.S. consumers aged 18 and older who actively engage with digital platforms. The survey was distributed through the Le Moyne College student email system and via public posts on two distinct Facebook and LinkedIn accounts. Data collection occurred between March 29 and April 23, 2023.

The questionnaire consisted of four sections:

1. **Demographic Information:** Collected participant details such as gender, age, ethnicity, and education level.
2. **Online Privacy Concerns:** Measured consumer apprehensions regarding digital privacy.

3. **Psychological Safety Perceptions:** Assessed feelings of security in online interactions.
4. **Brand Loyalty:** Examined attitudes toward brand trust and switching behaviors.

A total of 239 valid responses were analyzed. The sample comprised 64.6% female, 34.1% male, and 1.3% non-binary participants. The age distribution was as follows: 18-24 (52.6%), 25-34 (16.2%), 35-44 (9.4%), 45-54 (9.7%), 55-64 (7.5%), and 65+ (4.5%). Ethnic composition included 83.1% White/Caucasian, 4.9% Black/African American, 3.2% Asian/Pacific Islander, 2.9% Hispanic/Latino, 4.2% multiple ethnicities, and 1.3% other. Educational attainment ranged from high school diploma (36.4%) to bachelor's (34.7%), master's (16.2%), and doctoral degrees (2.3%).

MEASURES

Online Privacy Concerns

Consumer privacy concerns were assessed using the **Online Privacy Concern Scale (OPCS)** (Masur, 2018), which evaluates privacy anxieties from **vertical** (institutional) and **horizontal** (peer-related) perspectives. Due to survey length constraints, horizontal privacy concerns related to information sharing were excluded. Responses were recorded on a **7-point Likert scale** (1 = Not at all concerned to 7 = Very concerned), with higher scores indicating stronger privacy concerns.

Psychological Safety Perceptions

Psychological safety was measured using the **Neuroception of Psychological Safety Scale (NPSS)** (Morton et al., 2022), a validated instrument informed by **Polyvagal Theory**. This scale captures psychological safety across three subscales: **Compassion, Social Engagement, and Bodily Sensations.** For this study, only the Compassion and Social Engagement subscales were utilized. Responses were recorded on a **5-point Likert scale** (1 = Strongly disagree to 5 = Strongly agree), with higher scores reflecting increased psychological safety.

Brand Loyalty

Brand loyalty was assessed through a combination of **open-ended responses** and **two 5-point Likert scales.** Participants identified a brand they are loyal to and explained their reasons for loyalty. One scale (1 = Extremely unlikely to 5 = Extremely likely) measured the impact of brand safety perception on switching behaviors and privacy protection efforts. Another scale (1 = Not knowledgeable at all to 5 = Extremely knowledgeable) assessed consumer awareness of adjusting privacy settings across devices.

Scores for each measure were calculated using sum or mean values. Open-ended responses were analyzed for recurring themes. Survey items are detailed in **Appendices 1–3**.

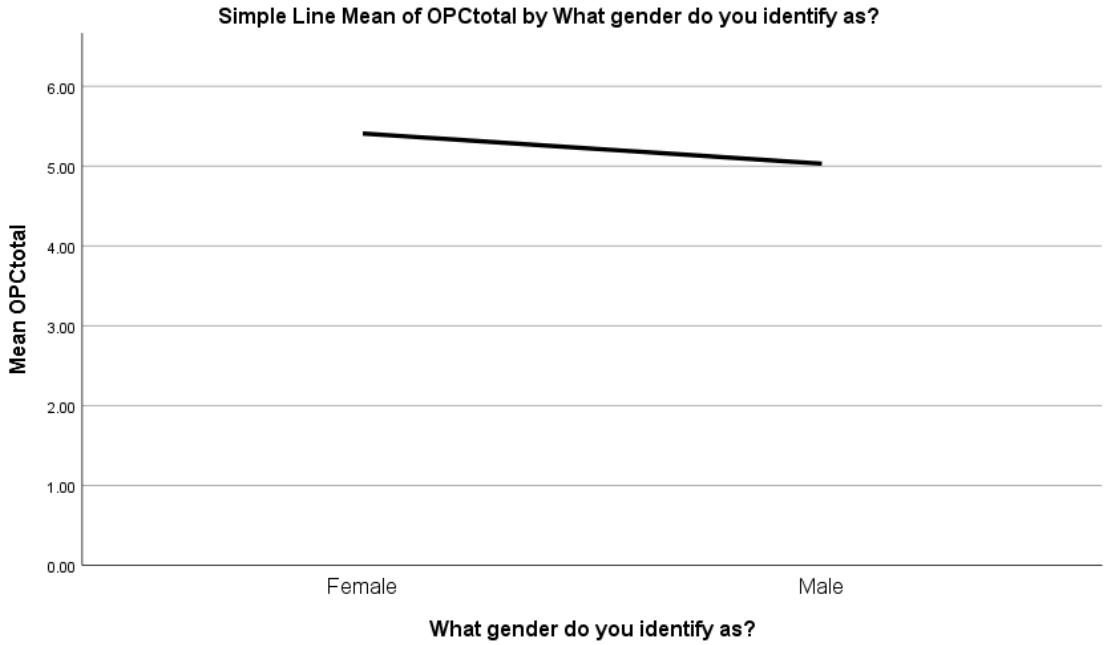
Data Analysis:

Consumer Data Privacy Concerns

The OPCS was leveraged to understand consumer data privacy concerns from vertical and horizontal perspectives. We calculated the total mean of the items using a 7-point scale to measure feelings of concern. The research uncovered respondents are concerned (M = 5.27) and horizontal privacy concerns (M = 5.43), or those involving other people, are higher than vertical privacy concerns of those involving websites (M = 5.14) or institutions (M = 5.16). Using an Independent Samples T-Test, the means statistically differ between horizontal and vertical privacy concerns ($p = 0.03$). Respondents reported feeling most concerned about 1. Someone misusing your identity on the internet (M = 5.81) 2. Other people getting information about you without your consent (M = 5.67) and 3. Not having insight into what institutions, public agencies, or intelligence services do with your data (M = 5.52). This confirms that consumers are concerned about their online privacy, with emphasized concerns about information access and theft involving other people.

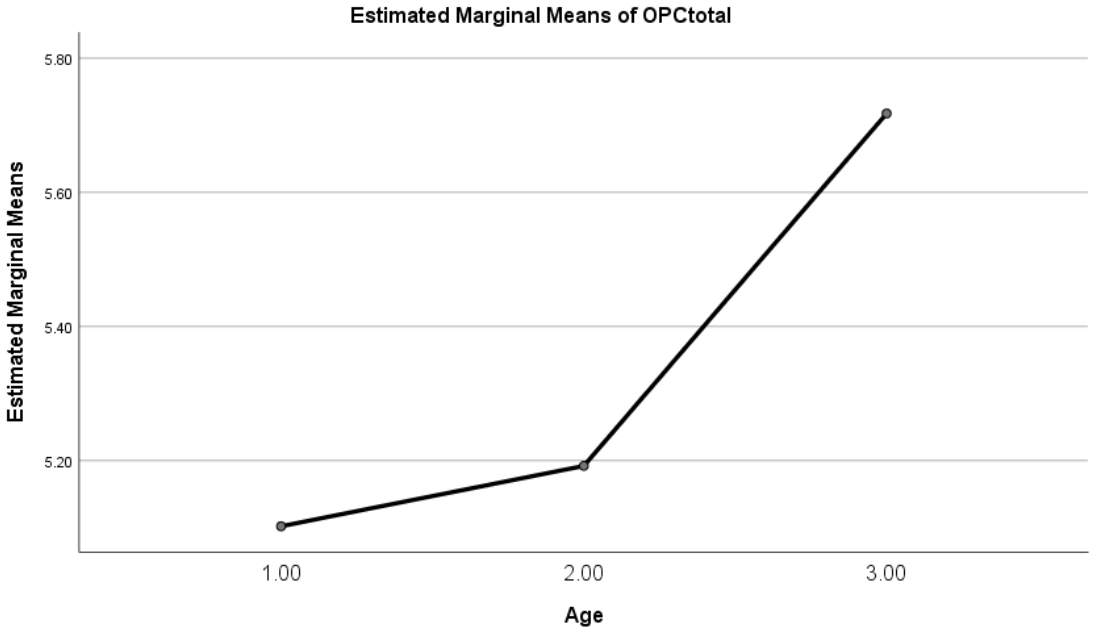
We then set out to understand if there are intricacies to consumer online privacy concerns, assessing against the respondents' personal information of gender, age, and level of education. Using an Independent Samples T-Test, there is a statistically significant relationship between gender and level of concern ($p = 0.01$) with Females (M = 5.40) feeling more concerned than Males (M = 5.03).

FIGURE 1



Using a Univariate Analysis of Variance Between-Subjects, there is a statistically significant relationship between age and level of concern ($p = 0.002$) where you become more concerned as you get older: 18-24 ($M = 5.10$), 25-44 ($M = 5.19$), and 45+ ($M = 5.71$).

FIGURE 2



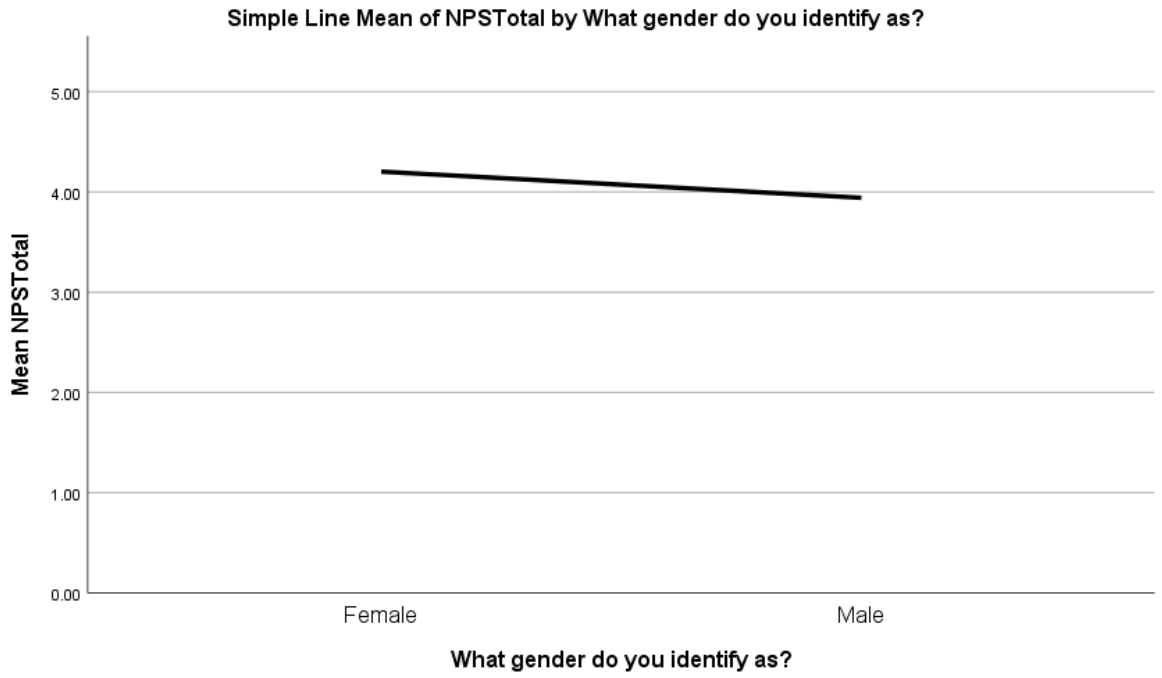
Using an Independent Samples T-Test, there is not a statistically significant relationship between education level and level of concern (p = 0.19). These indicate consumers are presently concerned overall with Females and older consumers displaying a higher level of concern.

Consumer Safety Perceptions

The NPSS was leveraged to test consumer safety perceptions, including Social Engagement and Compassion subscales. Using a 5-point Likert scale to measure feelings of psychological safety, we calculated the total mean of the items. The research uncovered respondents do feel safe overall (M = 4.11) as well as on the subscales of Social Engagement (M = 4.03) and Compassion (M = 4.18). Respondents are most likely to identify the following when they feel safe 1. There was someone I could trust (M = 4.29) 2. I felt compassion for others (M = 4.29) 3. I felt like I could comfort a loved one (M = 4.28). Anecdotally, those all involve another person, which stokes the question of how personal relationships impact feelings of safety. These disprove our assumptions by identifying most consumers do presently feel safe.

Additionally, we tested for nuances on consumer safety perceptions, assessing against the respondents' personal information. Using an Independent Samples T-Test, there is a statistically significant relationship between gender and safety perceptions (p = 0.001) with Females (M = 4.20) feeling less safe than Males (M = 3.94).

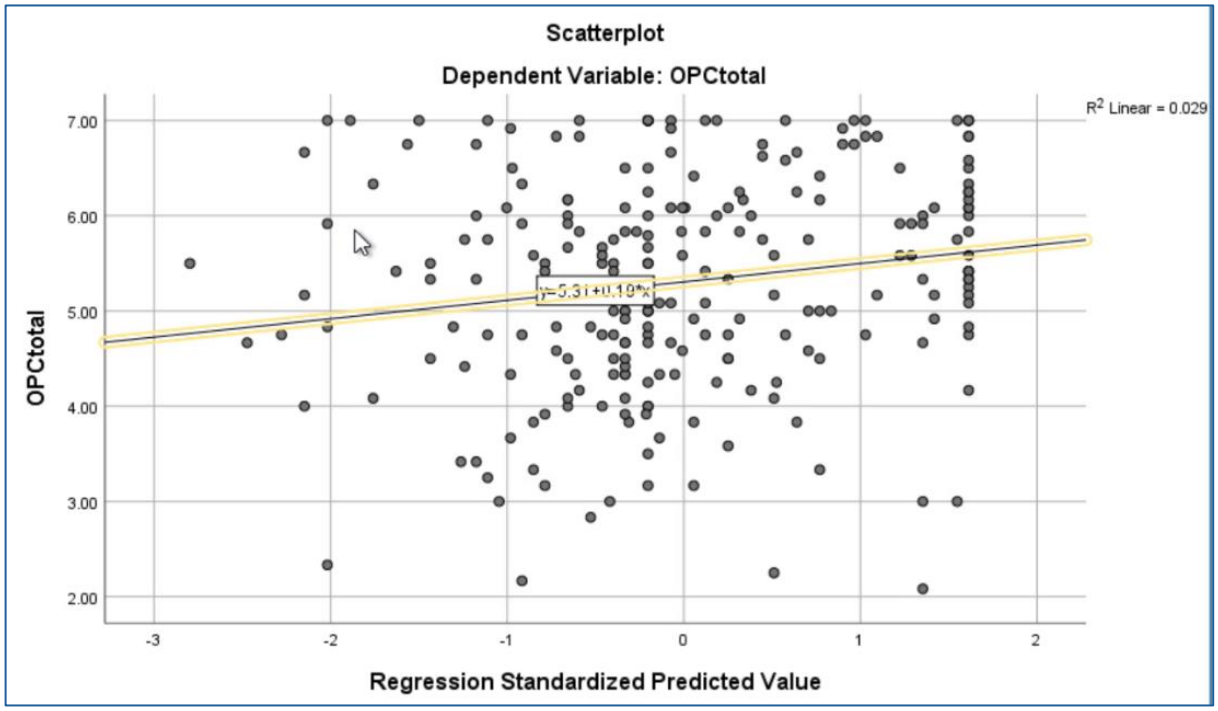
FIGURE 3



Using a Univariate Analysis of Variance Between-Subjects, there is not a statistically significant relationship between age and safety perceptions (p = 0.33). A Univariate Analysis of Variance Between-Subjects shows no statistically significant relationship between education level and safety perceptions (p = 0.83). These confirm consumers presently feel safe regardless of personal characteristics, except for Females who feel less safe than Males.

Finally, we set out to determine if there is a relationship between consumer feelings of safety and online privacy concerns. Using an ANOVA Regression analysis, there is a statistically significant relationship between respondent safety perceptions and online privacy concerns (p = 0.008); the higher the safety perceptions, the higher the level of concern.

FIGURE 4



This confirms a relationship exists but is opposite to what was hypothesized. Based on these findings:

H1: *Hypothesis 1 has been disproven in that although there is a relationship, those with higher safety perceptions also had higher online privacy concerns.*

Consumer Brand Loyalty

A series of questions were posed to understand consumer brand loyalty. The first question of this section was free form, asking respondents to name a brand they are loyal to with the highest frequencies being 1. Apple (N = 27) 2. Nike (N = 11) and 3. Lululemon (N = 6) and Target (N = 6). The second question used a 5-point scale to test how this brand makes respondents feel with respondents identifying feeling 1. Happy (M = 4.27) and 2. Confident (M = 4.02). Respondents reported this brand making them feel Safe as neither likely nor unlikely (M = 3.59). Similarly, they also reported this brand making them feel Secure as neither likely nor unlikely (M = 3.75). The third question was free form to tell us why they are loyal to that brand with the most common responses mentioning quality (N = 48), price (N = 17), comfort or comfortable (N = 12), service (N = 11), reliability (N = 11), and consistency (N = 11). Safe was used to describe the brand they were loyal to (N = 4) about car brands, a product used on animals, and a retailer who offered products in support of food allergies. This refutes our presumption that feelings of safety can yield brand loyalty and confirms:

H2: *Hypothesis 2 has been disproven as most respondents did not associate safety with the brand they are loyal to.*

Furthermore, we tested for likelihood to switch brands across various factors using a 5-point scale. Respondents reported being likely to switch brands if the brand is 1. Sharing direct messages (M = 4.38) 2. Sharing personal photos (M = 4.29) and 3. Sharing current location (M = 4.15). The results illustrated respondents are more likely to switch brands due to information sharing without their knowledge than a Decrease in quality (M = 3.94), Decrease in customer service (M = 3.26), or price increase (M = 2.74). The

exception was Sharing product usage, which resulted in neither likely nor unlikely (M = 3.28). This suggests that consumers are somewhat or extremely likely to switch brands if they discover private information sharing is occurring without their knowledge and thus:

H3: *Hypothesis 3 has been proven with three out of the four variables scoring as somewhat likely to switch brands (M = $\geq$ 4). These means were also higher than other transactional indiscretions.*

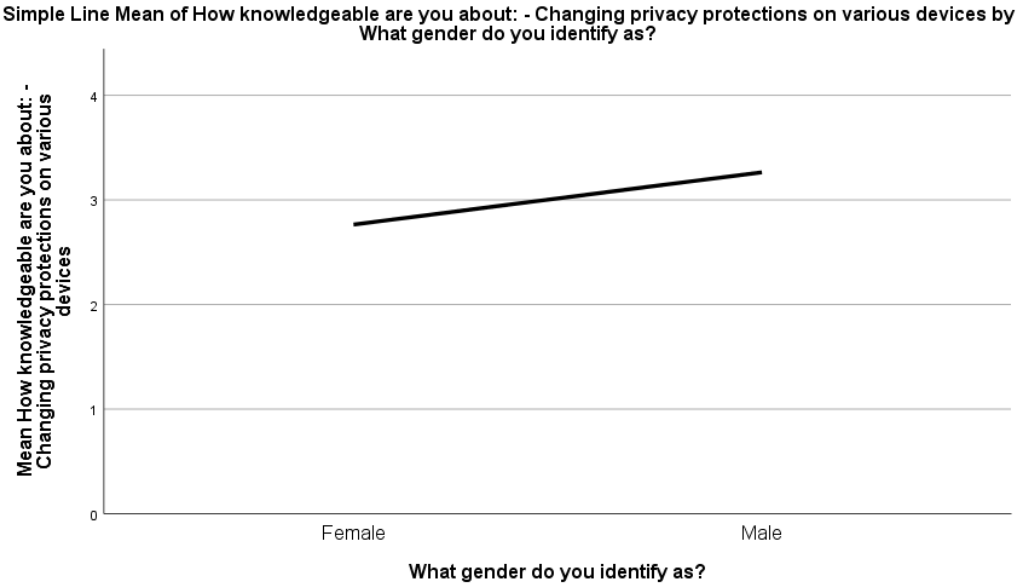
In terms of personal characteristics, using an Independent Samples T-Test, there is not a statistically significant relationship between gender and likelihood of switching brands for the following information sharing: Personal photos (p = 0.12), Direct messages (p = 0.49), and Personal usage data (p = 0.20). There is a statistically significant relationship between gender and likelihood of switching brands for Current location (p = 0.02) where Females (M = 4.29) are more likely to switch brands than Males (M = 3.93). Using an Independent Samples T-Test, there is not a statistically significant relationship between age and likelihood of switching brands for the sharing of Personal photos (p = 0.74), Direct messages (p = 0.25), Current location (p = 0.52), and Personal usage data (p = 0.29). Using an Independent Samples T-Test, there is not a statistically significant relationship between level of education and likelihood of switching brands except Increase in price (p = 0.01). Those with less than a college degree reported being neither likely nor unlikely to switch brands (M = 2.96) whereas those with a college degree or higher level of education reported being somewhat unlikely (M = 2.57) if the price were to increase. These demonstrate that consumers are likely to switch brands regardless of personal characteristics, apart from a few nuances.

Privacy Protection Knowledge & Pursuits

We continued leveraging a 5-point scale to test for the likelihood of pursuing privacy protections. Respondents answered they are neither likely nor unlikely to pursue privacy protections overall (M = 3.60) and are most likely to ignore unwanted digital ads (M = 4.39). We then reviewed privacy protection behaviors against personal characteristics. Using an Independent Samples T-Test, there is not a statistically significant relationship between gender and whether they are likely to pursue the following privacy protections: Change privacy settings on the device (p = 0.99), Change privacy settings on that company website (p = 0.80), Choose not to visit that company website again (p = 0.08), Read the company's privacy policy (p = 0.65), and Set up ad blockers (p = 0.07). There is a statistically significant relationship between gender and whether they are likely to Ignore unwanted digital ads (p = 0.02) where Males (M = 4.58) are more likely than Females (M = 4.28). Using an Independent Samples T-Test, there is not a statistically significant relationship between age and pursuing the following privacy protections: Change privacy settings on the device (p = 0.39), Choose not to visit that company website again (p = 0.18), Read the company's privacy policy (p = 0.19), and Ignore unwanted digital ads (p = 0.92). There is a statistically significant relationship between age and Change privacy settings on that company website (p = 0.03) and Set up ad blockers (p = 0.01) where those 45+ (M = 4.04) are more likely to Change privacy settings on that company website than 18-24 (M = 3.61) and those 45+ (M = 3.93) are more likely to Set up ad blockers than 18-24 (M = 3.45). Also, using an Independent Samples T-Test, there is not a statistically significant relationship between education level and whether they pursue privacy protections (p = 0.31). With a few nuances, this compounds other research that most consumers are unlikely to pursue privacy protections regardless of personal characteristics.

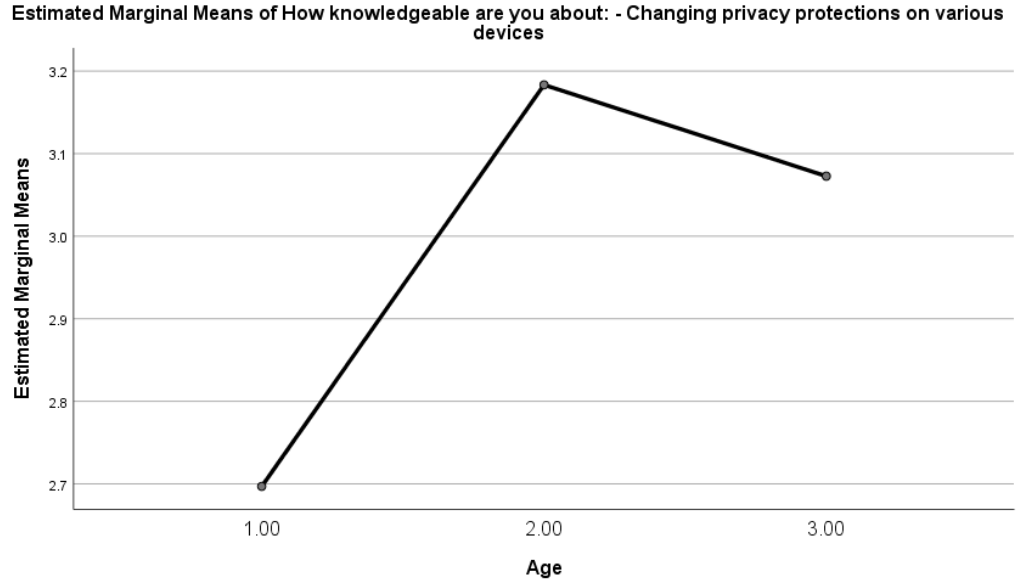
Finally, we used a 5-point scale to test respondent knowledge on changing privacy protections on various devices. Respondents felt moderately knowledgeable about changing privacy settings on various devices (M = 2.93). Using an Independent Samples T-Test, there is a statistically significant relationship between gender and privacy protection knowledge (p = 0.002) with Males (M = 3.26) feeling more knowledgeable than Females (M = 2.76).

FIGURE 5



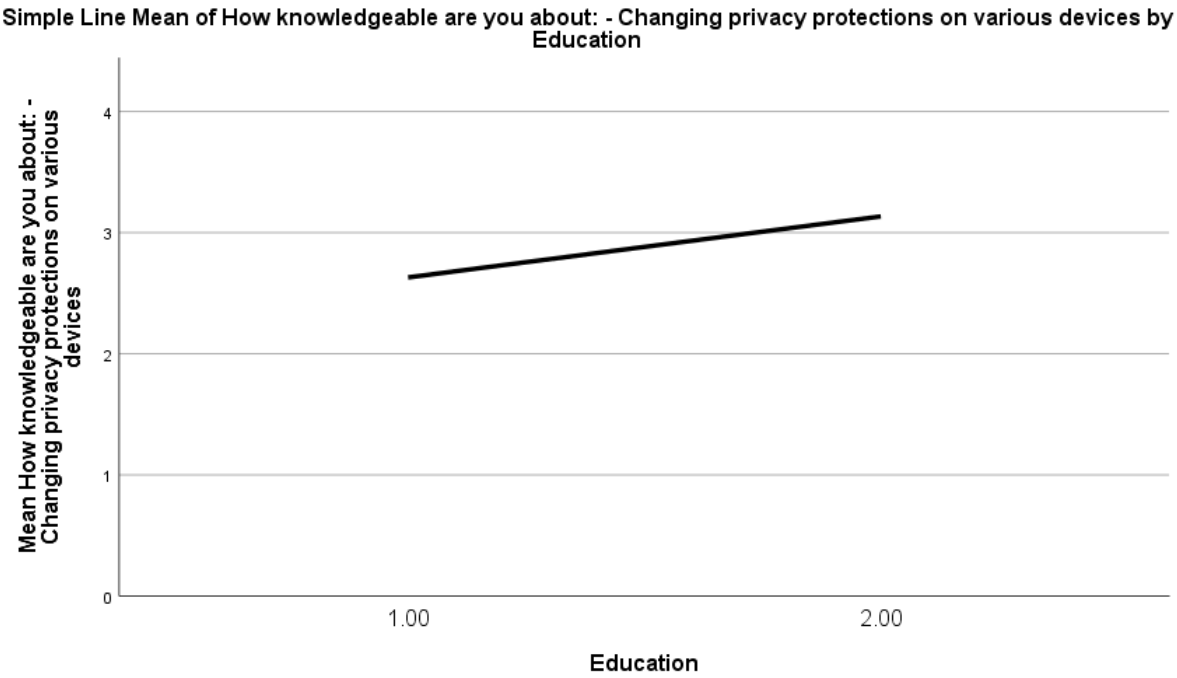
Using a Univariate Analysis of Variance Between-Subjects, there is a statistically significant relationship between age and privacy protection knowledge (p = 0.01) with those 18-24 (M = 2.69) feeling the least knowledgeable, 25-44 (M = 3.18) feeling the most knowledgeable, and 45+ (M = 3.07) feeling slightly less knowledgeable.

FIGURE 6



Using an Independent Samples T-Test, there is a statistically significant relationship between education level and privacy protection knowledge (p = 0.001) where those with a college degree or higher level of education (M = 3.12) feel more knowledgeable than those without a college degree (M = 2.63).

FIGURE 7



These also align with other forms of research, demonstrating consumers are not confident in their knowledge of privacy protections with Female, younger, and less educated consumers feeling the least knowledgeable.

RESULTS

The results of this study offer a clearer understanding of consumer data privacy concerns, safety perceptions, brand loyalty, and privacy protection behaviors in the current digital landscape. Specifically, consumers express significant concern about their online privacy, with personal photos, direct messages, and current location being the types of information they consider private and do not wish to be captured or shared by companies. Despite these concerns, however, consumers report feeling generally safe.

When it comes to brand loyalty, consumers prioritize factors such as product quality, price, comfort, service, reliability, and consistency. Brands that elicit loyalty make consumers feel happy and confident. However, loyalty is also heavily contingent upon transparency regarding how personal data is collected and shared. Any company activity perceived as a breach of privacy can impact consumer loyalty, potentially leading to brand switching. Interestingly, consumers tend to switch brands in response to privacy violations rather than taking protective actions, as they often feel uninformed about how to modify their privacy settings. This dynamic is likely to persist unless the consumer-brand data exchange relationship evolves.

Consumers should take proactive steps to educate themselves about data protection measures to mitigate online privacy concerns. Simply discontinuing or switching brands is neither a sustainable nor effective long-term solution for preserving privacy. Additionally, the lack of privacy protection actions tends to correlate with higher levels of online privacy concern. To address this, brands must prioritize earning digital trust by being transparent about their data collection and sharing practices. This transparency should include developing clear and accessible data privacy options. Given the potential consequences of privacy breaches, brands should consider minimizing the amount of personal information requested from consumers, limiting requests to only what is necessary for their products or services. Furthermore, brands

should establish robust security infrastructures, as identity theft and similar incidents can severely erode trust and lead to loss of business.

IMPLICATIONS

Upon reflection, several limitations of the study were identified. A larger, more diverse respondent sample would have strengthened the analysis, especially concerning safety perceptions. The homogeneity of the respondent ethnicities limited the ability to assess the influence of ethnicity on online privacy concerns, safety perceptions, brand loyalty, and privacy protection behaviors. Additionally, we had to group respondents by age and education level to ensure a sufficient sample size for analysis, which constrained the ability to explore these variables at more granular levels.

This study is the first to combine the OPCS and NPSS scales to explore the intersections of data privacy concerns, safety perceptions, and brand loyalty, highlighting several areas for future research. These include adding questions to identify whether respondents have experienced identity theft, as this could significantly impact privacy protection actions and safety perceptions. Modifying the NPSS to include questions specifically about digital properties, such as "Please rate how well the following statements describe your feelings during your experiences on digital platforms in the last week," could more directly link safety perceptions to data privacy concerns, potentially yielding different insights. Additionally, given the high tolerance for unwanted digital ads—often ignored by consumers—considering more invasive forms of privacy violations could further test the relationship between privacy protection actions and brand loyalty.

Further research could also explore the industry implications by incorporating questions about data privacy thresholds, brand loyalty, switching costs, and consumer sentiment. Understanding how these factors vary across industries will provide valuable insight into the broader landscape of privacy concerns. Another avenue for exploration is the concept of "irreplaceable" brands—those that consumers feel they cannot easily substitute. Research could investigate how reliance on certain products or services influences data privacy thresholds and protection behaviors.

Lastly, the primary objective of this study was to provide an updated understanding of data privacy concerns, safety perceptions, and brand loyalty. Continued research in these areas is essential to monitor the long-term effects of the ongoing data privacy crisis and the consequences of global events that impact consumer attitudes toward online safety and privacy.

REFERENCES

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020, April 27). *The consumer-data opportunity and the privacy imperative.* McKinsey & Company. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Balapour, A., Nikkhah, H.R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*(6221), 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Boehm, J., Grennan, L., Singla, A., & Smaje, K. (2022, September 12). *Why digital trust truly matters*. McKinsey & Company. Retrieved from https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

Boudet, J., Huang, J., Rathje, K., & Sorel, M. (2019, November 7). *Consumer-data privacy and personalization at scale: How leading retailers and consumer brands can strategize for both*. McKinsey & Company. Retrieved from https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/consumer-data-privacy-and-personalization-at-scale

Insurance Information Institute. (2022). *Facts + Statistics: Identity theft and cybercrime*. Retrieved from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

Klosowski, T. (2021, September 6). The State of Consumer Data Privacy Laws in the US (And Why it Matters). *The New York Times Wirecutter.* Retrieved from https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Masur, P.K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-78884-5

Melumad, S., & Meyer, R. (2020). Full disclosure: How smartphones enhance consumer self-disclosure. *Journal of Marketing*, *84*(3), 28–45. https://doi.org/10.1177/00222429209127

Morton, L. (2022, October 22). Psychological safety during uncertain times. *Psychology Today*. Retrieved from https://www.psychologytoday.com/us/blog/psychologically-informed-medicine/202210/psychological-safety-during-uncertain-times

Morton, L., Cogan, N., Kolacz, J., Calderwood, C., Nikolic, M., Bacon, T., . . . Porges, S.W. (2022). A new measure of feeling safe: Developing psychometric properties of the Neuroception of Psychological Safety Scale (NPSS). *Psychological Trauma: Theory, Research, Practice, and Policy*. Advance online publication. https://doi.org/10.1037/tra0001313

N.G., A. (2023, February 22). The raucous battle over Americans' online privacy is landing on states. *Politico*. Retrieved from https://www.politico.com/news/2023/02/22/statehouses-privacy-law-cybersecurity-00083775

Pew Research Center. (2019, November 15). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

PwC. (2022). *Creating loyalty in volatile times. PwC Customer Loyalty Survey 2022*. Retrieved from https://www.pwc.com/us/en/services/consulting/business-transformation/library/customer-loyalty-survey.html

Segal, E. (2022, October 21). The latest attempt to address the online data and privacy crisis. *Forbes*. Retrieved from https://www.forbes.com/sites/edwardsegal/2022/10/21/the-latest-attempt-to-address-the-online-data-and-privacy-crisis/?sh=30bae47c34e4

Singer, N. (2019, November 2). The government protects our food and cars. Why not our data? *The New York Times*. Retrieved from https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html

Statista Research Department. (2021). *Ad blocking user penetration rate in the United States from 2014 to 2021.* Statista. Retrieved from https://www.statista.com/statistics/804008/ad-blocking-reach-usage-us/

Tang, J., Akram, U., & Shi, W. (2021). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. *Journal of Enterprise Information Management*, *34*(4), 1097–1120. https://doi.org/10.1108/JEIM-03-2020-0088

Tian, X., Chen, L., & Zhang, X. (2022). The role of privacy fatigue in privacy paradox: A PSM and heterogeneity analysis. *Applied Sciences*, *12*(19), 9702. https://doi.org/10.3390/app12199702

Wottrich, V.M., Van Reijmersdal, E.A., & Smit, E.G. (2019). App users unwittingly in the spotlight: A model of privacy protection in mobile apps. *The Journal of Consumer Affairs*, *53*(3), 1056–1083. https://doi.org/10.1111/joca.12218

APPENDIX

TABLE 1
ONLINE PRIVACY CONCERN SCALE (OPCS)

Vertical	**How concerned are you about**
Factor 1a: about website providers	Website or app providers recording and using your surfing behavior?
	Website or app providers sharing your data with unknown third parties?
	Website or app providers tracking your online behavior and thereby getting information about you?
Factor 1b: about institutions	Institutions, public agencies, or intelligence services monitoring your online communication?
	Not having insight into what institutions, public agencies, or intelligence services do with your data?
	Institutions, public agencies, or intelligence services collecting and analyzing the data that you share on the Internet?
Horizontal	
Factor 2a: about information access	Other people getting information about you without your consent?
	Other people finding information about you online?
	Other people search information spying on you on the Internet?
Factor 2b: about identity theft	People on the Internet not being who the claim to be?
	An unknown person claiming to be you on the Internet?
	Someone misusing your identity on the Internet?

TABLE 2
NEUROCEPTION OF PSYCHOLOGICAL SAFETY SCALE (NPSS)

Subscale	**Item**
Social Engagement	I felt valued
	I felt comfortable expressing myself
	I felt accepted by others
	I felt understood
	I felt like others got me
	I felt respected
	There was someone who made me feel safe
	There was someone that I could trust
	I felt comforted by others
	I felt heard by others
	I felt like people would try their best to help me
	I felt cared for
	I felt wanted
	I didn't feel judged by others
Compassion	I felt able to empathize with other people
	I felt able to comfort another person if needed
	I felt compassion for others
	I wanted to help others relax
	I felt like I could comfort a loved one
	I felt so connected to others I wanted to help them
	I felt caring

TABLE 3
BRAND LOYALTY

Name a brand you are loyal to	Free Form
For each of the following, how likely is this brand to make you feel?	Happy
	Safe
	Used
	Confident
	Embarrassed
	Secure
In your own words, please tell us why you are loyal to that brand	Free Form
For each of the following, how likely are you to switch brands?	Increase in price
	Decrease in quality
	Decrease in customer service
How likely are you to switch brands if the company was sharing each of the following types of information about you without your knowledge?	Personal photos
	Direct messages
	Current location
	Product usage data
Upon using a website you discover the company is sharing your data with a third-party and you begin seeing unwanted digital ads. How likely are you to pursue the following privacy protections:	Change privacy settings on the device
	Change privacy settings on that company website
	Choose not to visit that company website again
	Read the company's privacy policy
	Set up ad blockers
	Ignore unwanted digital ads
How knowledgeable are you about:	Changing privacy protections on various devices