Quantifying Data Privacy Proficiency: An Analysis of Data-Sharing Behavior and Data Privacy Concerns among Digital Consumers

Angel D. Leal[1]
Isabela State University-Cauayan City Campus, Philippines

Marvin L. Ramirez
Isabela State University-Cauayan City Campus, Philippines

ARTICLE HISTORY
Date Submitted: September 27, 2025 | ***Date Accepted:*** November 14, 2025 | ***Date Published:*** December 30, 2025

ABSTRACT

In the Philippines, where online transactions and social media usage are widespread, safeguarding digital privacy is crucial for consumer protection. Existing studies have extensively explored data privacy concerns and behaviors in urban and international contexts. However, there is a lack of empirical studies that assess data privacy proficiency and its behavioral determinants among digital consumers in the Philippines, especially in provincial settings such as Cauayan City, Isabela. This study then assessed the data privacy concerns and data-sharing behaviors of digital consumers in Cauayan City. It also sought to determine how attitude, subjective norms, and perceived behavioral control influence their intention to share personal data, using the Theory of Planned Behavior as the study framework. A descriptive-correlational research design was employed. A structured questionnaire was administered to 500 respondents who regularly engage in online transactions. Data were analyzed using descriptive statistics, Pearson correlation, and multiple regression analysis. Findings indicated that, while consumers are moderately to highly concerned about data privacy, they continue to share personal data such as names, contact information, and addresses on platforms like Facebook, GCash, and Shopee. Results also showed that attitude and subjective norms significantly influence data-sharing intention, while perceived behavioral control has a weaker effect. This reflects the "privacy paradox" phenomenon, where expressed concern does not translate into cautious behavior. This study concludes that digital consumers in Cauayan City demonstrate moderate data privacy proficiency, but their behavior often prioritizes convenience and trust in platforms over caution.

Keywords: data privacy; digital consumers; data-sharing behavior; privacy paradox; Theory of Planned Behavior

I. INTRODUCTION

doi: 10.5281/zenodo.18081626
[1]Corresponding author: lealangeld@gmail.com

Data privacy is fundamentally the right of an individual to control their personal information, specifically how it is collected, used, and disclosed, alongside the implementation of security and protocols by organizations that process this data (Komnenic, 2025). In this context, data privacy proficiency refers to the knowledge of digital consumers regarding their personal data and data privacy principles. Its primary function is to safeguard personal information from unauthorized access, exploitation, or abuse, including identity theft and fraud.

In the current data-driven world, the significance of data privacy has grown immensely (Stallings, 2020). It upholds the fundamental right to privacy (Norberg et al., 2007) and personal integrity, which is essential as technology advances and digitalization intensifies. When individuals are confident that their personal data is handled securely and ethically, they are more willing to engage with organizations and share necessary information (Solove, 2004). Furthermore, robust data privacy practices are critical for establishing and sustaining excellent customer relationships (Winer, 2001) by promoting trust in digital interactions (Tobin, 2024).

Despite the numerous benefits derived from sharing information online, such as enjoying the features of digital services, this practice introduces significant concerns, including data breaches, misuse of information, and unauthorized third-party sharing. A critical example occurred in the Philippines in 2023 when the Philippine Health Insurance Corporation (PhilHealth) suffered a major cybersecurity incident. Hackers, identified as Medusa, accessed and began releasing 734 GBs of stolen data on the dark web, which included confidential memos and member data like addresses, phone numbers, and insurance IDs (Samaniego, 2023). This incident highlights the acute vulnerability of personal data, even within government institutions.

This concern is widely shared by the Filipino populace. A Consumer Pulse Survey in Q2 of 2024 indicated that a striking 89% of the 944 surveyed Filipinos expressed concern about sharing their personal information, underscoring a growing apprehension over shared data despite the digital benefits they receive in exchange (Gonzales, 2024).

Despite the extensive international research concerning the privacy concerns of digital consumers, studies focusing specifically on the Philippine setting remain limited. This creates a critical research gap, as factors like demographics and cultural nuances that influence consumer perceptions and data-sharing practices in other countries may not translate directly or accurately to the Filipino context. Therefore, this study aims to address this lack of local knowledge by focusing specifically on Filipino digital consumers.

This research will employ a descriptive correlational quantitative approach to analyze the core factors influencing consumer behavior. Specifically, the objectives are to assess the perceptions of digital users regarding data privacy and their willingness to share personal information online; to examine the impact of attitude, subjective norms, perceived behavioral control, and intention on the data-sharing practices of Filipino consumers and their overall level of data privacy concern; and to determine how various demographic characteristics (age, gender, profession, educational background, and geographic location) influence these concerns.

By focusing on these specific variables within the Philippine demographic, the study promises to provide valuable, context-specific insights into consumer behavior and effective data governance practices in the digital age.

II. METHODS

A. Research Design

The researchers employed a descriptive correlational quantitative approach, which is ideal for studies aiming to capture a snapshot of a situation while also investigating the relationship between variables. This technique, as noted by McBurney and White (2009), allows for the collection of data that provides a static description of the current circumstances. In the context of this study, this approach was crucial for analyzing the attitudes, subjective norms, and perceived behavioral intentions of digital consumers concerning their data-sharing intentions and the subsequent impact on their data privacy concerns.

To achieve such, the study utilized surveys to systematically gather statistical information on consumers' privacy concerns and behaviors. This method of collecting quantitative data ensured an in-depth understanding of the digital consumers' disposition toward data privacy by quantifying their attitudes and establishing how these factors correlate with their behavioral intentions regarding data sharing. The descriptive element provided the necessary static image of the consumers' existing mindset, while the correlational aspect allowed the researchers to determine the strength and direction of the relationships between the psychological constructs (like attitude and subjective norms) and the behavioral outcomes (like data-sharing intention and privacy concerns).

This choice of methodology is strategic because it moves beyond simply describing the existence of data privacy concerns; it seeks to identify predictors or associated factors that influence a consumer's decision to share or withhold personal data. By statistically analyzing the collected data, the researchers can generate empirical insights into the complex interplay between psychological drivers and privacy-related behaviors, offering a robust, quantitative foundation for understanding and addressing data privacy issues in the digital consumer landscape.

B. Research Instrument

The research was structured around a descriptive correlational approach, a quantitative method central to the study's design. This approach, as noted by Creswell (2014), is characterized by observing and measuring the relationships between variables without any manipulation by the researchers. The goal is to describe the characteristics of a population and determine the extent to which two or more variables are statistically associated. All the necessary data for this analysis were gathered through closed-ended questions, ensuring that responses were suitable for quantification and subsequent statistical analysis.

The principal method for data collection involved using a structured survey questionnaire, which was administered both in a physical format and via a Google Form to accumulate quantitative data from the respondents. This survey was systematically

divided into six main parts to capture both demographic context and the core psychological constructs under investigation. The first part collected the demographic profile of the participants. The second part consisted of select questions addressing specific data-sharing behaviors, categorized into four sub-groups: the type of information usually shared, the platforms used for sharing, the duration since they last shared personal data online, and whether they granted permission for the site or platform to use, collect, process, and store their shared data.

The remaining sections were dedicated to measuring the core variables: the participants' attitude, subjective norms, perceived behavioral control, and intention toward data-sharing and data privacy concerns, respectively. To measure these nuanced constructs effectively, respondents answered these sections using a five-point Likert Scale. This scale ranged from 5 (Strongly Agree) down to 1 (Strongly Disagree), with 3 representing Neutral. The use of the Likert scale facilitates the conversion of qualitative opinions and feelings into quantitative data points, which is essential for conducting the correlational analysis to determine the strength of the relationship between these psychological factors and the ultimate decision to share data.

C. Data Analysis

The primary analytical strategy for this study was the use of descriptive statistics to examine the data collected from the participants. As Bhandari explains, descriptive statistics are essential for summarizing and organizing the characteristics of a dataset, which, in this context, are the responses and observations gathered from the sample population. This approach was highly appropriate for the research, as it allowed the researcher to quickly and clearly grasp the summary of participants' concerns and behaviors toward data privacy, effectively reducing large sets of data to a more manageable and understandable form.

To interpret the overall findings, especially regarding the level of attitude, subjective norms, and perceived behavioral control, the raw data from participant responses were systematically tallied, tabulated, analyzed, and interpreted. The key method employed in the treatment of this data was the computation of means for the responses. Calculating the mean provided a single, central value that represents the typical response for each variable. This was then used in conjunction with a predefined rating guide to interpret the overall level or range of the participants' feelings and intentions toward data-sharing and data privacy concerns.

Beyond descriptive analysis, this study also employed Multiple Regression Analysis to test the core hypotheses. Specifically, this statistical technique was used to determine if the constructs of the Theory of Planned Behavior (Attitude, Subjective Norms, and Perceived Behavioral Control) significantly predict the digital consumer's intention to share data. This analysis allowed the researchers to establish the strength, direction, and predictive contribution of each psychological factor on the dependent variable.

D. Instrument Validity and Reliability

To ensure the quality and rigor of the data collection, the research instrument underwent systematic validation and reliability testing. The survey questionnaire was first submitted for content validation to two registered psychometricians. Their expert review focused on the clarity, relevance, and appropriateness of the questions in measuring the intended psychological constructs (attitude, subjective norms, perceived behavioral control, and data-sharing intention). Their feedback was integrated to enhance the face and content validity of the instrument.

Following validation, a pilot test was conducted with 30 respondents whose demographics and characteristics closely mimicked the actual target population. This preliminary administration served to identify potential ambiguities in the questions, assess the clarity of the instructions, and finalize the data collection procedures before the main study.

The data gathered from the pilot test were used to establish the internal consistency and reliability of the scales through Cronbach's Alpha (α) testing. The calculated α coefficients for all scales demonstrated high internal consistency, exceeding the generally acceptable threshold of α=0.70. These high coefficients affirm that the items within each scale consistently measure the same underlying construct, thereby providing a reliable basis for the subsequent quantitative analysis.

III. RESULTS AND DISCUSSION

A. Profile of the Respondents

The study successfully surveyed a total of 500 digital consumers residing in Cauayan City. The demographic analysis, detailed in Table 1, reveals a clear profile of the sample.

Table 1.

Frequency and Percentage Distribution of Respondents according to Occupation, Age, and Gender of Digital Consumers in Cauayan City

Demographic Profile		Frequency	Percentage
Occupation	No answer	38	7.6
	Public	9	1.8
	Private	103	20.6
	Student	343	68.6
	Others	7	1.4
Age of Respondents	20 or less	200	40.0
	21 to 30	236	47.2
	31 to 40	29	5.8
	41 to 50	17	3.4
	over 50	7	1.4
	No answer	11	2.2
Gender	Female	299	59.8
	Male	188	37.6
	No answer	13	2.6

TOTAL	500	100.00

Note: Percentage may not equal 100% due to rounding errors.

In terms of occupation, students constituted the largest segment, accounting for 68.6% (n=343) of the total sample. Conversely, the "others" category, primarily composed of self-employed individuals, represented the smallest group at only 1.4% (n=7). Regarding age distribution, nearly half the respondents belonged to the 21–30 age bracket, comprising 47.2% (n=236). Similar to the occupational findings, the oldest cohort, those over 50 years old, was the least represented, making up only 1.4% (n=7). Finally, the sample exhibited a majority female presence, with women constituting 59.8% (n=299) of the respondents, followed by males at 37.6% (n=188). A small fraction of respondents (2.6%, n=13) chose not to disclose their sex.

B. Information Usually Shared Online

The study clearly demonstrated that digital consumers readily provide various types of personal information to utilize the features of online platforms. As detailed in Table 2, the most frequently shared piece of data is the Name, cited by a near-unanimous majority of respondents at 97.8% (n=489). This finding is consistent with research by Auxier and Anderson (2021), highlighting the necessity of a name as a fundamental identifier for facilitating social interactions and establishing accounts in the digital environment.

Table 2.

Frequency and Percentage Distribution of Respondents according to Information Usually Shared Online

Information Usually Shared Online	Frequency	Percent
Name	489	97.8 %
Address	406	81.2 %
Age	388	77.6 %
Phone Number	377	75.4 %
Email	289	57.8 %
Birthdate	269	53.8 %
Civil Status	214	42.8 %
Citizenship	174	34.8 %
Birth Place	170	34.0 %
ZIP Code	166	33.2 %
Occupation	157	31.4 %
Religion	141	28.2 %
Educational Attainment	117	23.4 %
ID Numbers	98	19.6 %
School Attended	91	18.2 %
Emergency Contact Information	82	16.4 %

College Degree	81	16.2 %
Dialect	81	16.2 %
Parents Full Name	68	13.6 %
Height	56	11.2 %
Blood Type	56	11.2 %
Ethnicity	52	10.4 %
Weight	51	10.2 %
Siblings Name	50	10.0 %
Bank Account Information	42	8.4 %
Children's Name	26	5.2 %
Saved Playlist	17	3.4 %
Others	2	0.4 %

Note: Percentage may not equal 100% due to rounding errors.

Following *Name*, other high-frequency items include *Address* and *Age*, reported by 81.2% (n=406) and 77.6% (n=388) of respondents, respectively. As suggested by Binns (2018), these are commonly required fields for functional necessities such as account verification, content customization (e.g., age-gating), fulfilling legal regulations, and processing e-commerce transactions, particularly when an address is needed for shipping.

Conversely, the data reveals a marked reluctance among consumers to share highly sensitive information. The least frequently shared items are Bank Account Information (8.4%, n=42), Children's Name (5.2%, n=26), and Saved Playlists (3.4%, n=17). The low rates of sharing for bank account information and children's names reflect a heightened awareness of risk, as both are generally considered sensitive personal information under the Republic Act No. 10173, or the Data Privacy Act of 2012. This legislation mandates stricter data protection for such categories, which likely contributes to the consumers' hesitancy to disclose them. The very low disclosure of saved playlists, while perhaps not legally classified as sensitive, suggests that consumers are cautious about sharing data that could reveal intimate details about their personal preferences and behavior, which can be easily leveraged for targeted profiling.

C. Platforms where Digital Consumers Usually Share their Personal Information

As the digital age continuously develops, online platforms play a huge role in everyone's life. Table 3 illustrates the online platforms that digital consumer usually shares their information with. The data are categorized according to the type of platforms, namely social media, online banking, e-wallet, e-commerce, search engines, entertainment, and communication.

In terms of social media platforms, Facebook took the largest percentage with 93.2% or 466 respondents. This finding coincides with the study from the Pew Research Center, which states that despite the emergence of other social media platforms, Facebook remains the most widely used because it maintains social and personal connections

among users (Auxier & Anderson, 2021). While the least used platform is the X, formerly known as Twitter, with only 19.2% or 96 respondents. This suggests that X is not a widely used platform to share personal information, as it is more focused on opinions, news, and real-time updates only.

As the banking business made its way to the online world, several banking apps have been created. *Landbank of the Philippines* emerges as the dominant online banking app, comprising 34.6% or 173 respondents. Going back to the demographic profiles, the majority of the respondents are students. This suggests that *Landbank* is the most used online banking app because this is the required bank to use for their scholarship, financial assistance, and stipend. *SeaBank*, on the other hand, acquired the lowest percentage with only 2.8% or 14 respondents. This finding suggests that only a few are aware of this bank because it was only introduced by a shopping platform in the Philippines.

For e-wallet platforms, *GCash* dominated in the e-wallet category, comprising 77.6% or 388 respondents. Studies show that *GCash* is the most convenient e-wallet platform that an individual can use. Individuals could complete their transaction easily with *GCash* as it simplifies their payment processes and it is more practical to use (Belmonte et al., 2024). Meanwhile, *PayPal,* with 7.6% or 38 respondents, is recorded as the least used. Compared to *GCash*, *PayPal* is a foreign e-wallet app. This implies that Filipinos are more inclined towards apps that are specifically generated for Filipinos.

The emergence of shopping platforms since the pandemic has given way to different e-commerce apps. *Shopee*, as the most widely used shopping platform in the Philippines, comprised 75.2% or 376 respondents in the study. According to the study of Bacay et al. (2022), creative sales promotion and timing attract consumers, especially during *Shopee's* big online shopping event. This implies that *Shopee*'s marketing strategy leads them to be the most-used shopping platform in the Philippines. On the contrary, *Shein* took the lowest percentage with only 19% or 95 respondents. While *Shein* offers a variety of clothing, this finding suggests that consumers are more inclined to shopping apps that offer a wide range of different products, like *Shopee*.

Under search engine platforms, *Google Chrome* took a large percentage, comprising 89% or 445 respondents. This finding may be due to what Azizan et al. (2018) concluded, that *Google Chrome* gives accurate search results for its users. *Bing*, on the other hand, got the lowest percentage with only 3.6% or 18 respondents. This is because of its later emergence in the market compared to *Google,* which has a stronger brand recognition because of its earlier market dominance.

When it comes to Entertainment platforms, YouTube has the greatest number of users, comprising 80% or 395 respondents, compared to *Bilibili* with only 27.6% or 138 respondents. Despite the popularization of Netflix, YouTube remains widely used, likely because of its free service. According to Mateo (2024) and Magadia (2025), more Filipinos prefer *YouTube* for information and entertainment making it the "new TV" of Filipinos. While *BiliBili* is left on track because of its late introduction in the market.

For Communication platforms, *Gmail* secured its dominance with 69.6% or 348 respondents. According to Zacholska- Majer (2025), *Gmail* has consistently raised the bar in terms of usability, innovation, and integration since its introduction in 2004. While

Viber got the least percentage with only 10.8% or 54 respondents, because of its limited range and being dominated by other globally known communication platforms. Overall, these findings illustrate a clear pattern of how digital consumers share their information online.

D. Timeframe of Last of Data-Sharing

Table 3 presents the timeframe of when was the last time the digital consumers last shared their data online. It was seen in the table that the majority of the respondents, comprising 32.4% or 162 respondents, do not remember the last time they shared their data online. While 31.4% or 157 respondents said that they share their data online one week ago. 8.4% or 42 respondents said that they share their data online las 2-3 months ago while 5.8% or 29 respondents, which is the least, answered 4-6 months ago.

Table 3.
Frequency and Percentage Distribution of Respondents by Time Since Last Sharing Personal Information Online

Recency of Sharing Personal Information Online	Frequency	Percent
Cannot remember	162	32.4 %
One week ago	157	31.4 %
A month ago	65	13.0 %
Two weeks ago	44	8.8 %
2-3 months ago	42	8.4 %
4-6 months ago	29	5.8 %
No answer	1	0.2 %
TOTAL	500	100.0%

Note: Percentage may not equal to 100% due to rounding errors.

E. Permission Granted to Platforms for the Use, Collection, Processing, and Storage of Shared Data

In Table 4, the permissions given to platforms to use, collect, process, and store digital consumers' shared data are presented.

Table 4.
Frequency and Percentage Distribution of Respondents by Permission Granted for Online Data Use and Storage

Consent to Online Data Use and Storage	Frequency	Percent
Yes	353	70.6 %
No	111	22.2 %
Not Aware	36	7.2 %
TOTAL	500	100.00

Note: Percentage may not equal to 100% due to rounding errors.

A total of 70.6 percent, or 353 respondent**s**, stated that they grant permission to platforms or sites to use, collect, process, and store their data. This indicates that users tend to grant permission to platforms in exchange for quality service, ease of use, privacy and security assurance seals**,** and a disposition toward third-party certification (Alzaidi & Agag, 2022). On the other hand, 22.5 percent**,** or 111 respondents**,** answered no, while 7.2 percent**, or** 36 respondents**,** indicated that they were not aware of this practice.

F. Attitude towards Data-Sharing Online and Data Privacy Concerns

As presented in Table 6, the analysis of participant responses yielded a mean score of 3.4 (SD=0.677) for Attitude Towards Data-Sharing Online. Positioned slightly above the neutral midpoint of the 5-point Likert scale, this mean score indicates that respondents hold a moderate to slightly positive attitude toward sharing data online.

Table 5.
Descriptive Statistics Attitude (N=500)

Construct	Mean	Std. Deviation	N
Attitude Towards Data-Sharing Online	3.4	0.677	500
Attitude Towards Data Privacy Concerns	3.96	0.664	500

This moderate overall attitude suggests that while digital consumers recognize and value the benefits and convenience offered by online platforms that require data input, their willingness to share personal information is accompanied by a degree of caution. Rather than indicating indifference, the score reflects a considered position in which perceived advantages are weighed against potential risks. This interpretation aligns with Marin et al. (2022), who found that users remain aware of data misuse and privacy violations even when they acknowledge the functional benefits of data-sharing. Similarly, Spanaki (2021) emphasized that willingness to share data is highly conditional, shaped by users' perceptions of data handling practices and their level of trust in specific platforms. In this context, the mean score of 3.4 can be understood as evidence of a strategic and risk-aware approach to online data-sharing.

In contrast, Table 5 shows that participants expressed markedly stronger concerns regarding data privacy, as reflected in the higher mean score of 3.96 (SD = 0.664) for Attitude Towards Data Privacy Concerns. This substantial difference between the two constructs highlights a key psychological tension in digital behavior. While respondents may be willing to share data in order to access online services, they simultaneously express significant concern about how their data is collected, processed, and used. This finding mirrors the contemporary digital environment described by Zuboff (2019), in which personal data is increasingly commodified, intensifying user awareness and concern. The elevated privacy concern score suggests a growing demand for accountability, control, and transparency in data practices. As Aragon et al. (2024) observed, although users may accept the exchange of personal information for

personalized services, this acceptance is increasingly contingent upon expectations of responsible data management and security.

The divergence between the two mean scores is particularly noteworthy. While attitudes toward data-sharing remained neutral to moderately positive (M = 3.4), concerns about data privacy were clearly stronger (M = 3.96). This discrepancy underscores a central tension in the digital consumer experience. Acceptance of data-sharing appears to be driven largely by pragmatic considerations such as convenience and access, rather than by a lack of concern for privacy. This pattern closely aligns with the Privacy Paradox described by Barnes (2006), whereby individuals engage in data disclosure despite holding persistent concerns about privacy risks and data security. Consumers, therefore, appear to navigate the digital environment through a calculated but uneasy trade-off between functionality and privacy assurance.

Table 6.
Descriptive Statistics for Attitude towards Data-Sharing Online

	Attitude Towards Data Sharing Online	Mean	SD	QD
1.	Comfort with Sharing Personal Data Online	3.32	1.016	Neutral
2.	Perceived Security of Data Shared with Reputable Companies	3.39	0.961	Neutral
3.	Willingness to Share Data for Improved Website or App Experience	3.41	0.955	Neutral
4.	Trust in Companies' Responsible Use of Shared Data	3.42	0.952	Neutral
5.	Lack of Concern About Online Data Use	2.76	1.149	Neutral
6.	Perceived Convenience of Online Data Sharing	3.09	1.069	Neutral
7.	Perceived Benefit–Risk Advantage of Online Data Sharing	3.25	1.087	Neutral
8.	Attention to Privacy Policies Before Sharing Data	3.84	0.996	Positive
9.	Willingness to Share More Data Under Stronger Privacy Regulations	3.83	0.942	Positive
10.	Likelihood of Sharing Personal Information with Trusted Online Platforms	3.63	0.987	Positive

Table 6 provides a more granular view of the respondents' attitude towards data-sharing online, and helps contextualize the overall mean score of 3.4, generally reinforcing the previously established finding of a neutral to slightly positive overall disposition (mean score of 3.4). A notable example of this moderate stance is reflected in Statement 8 which registered a relatively positive mean score of 3.84 (SD=0.996). This finding suggests that respondents recognize the importance of privacy policies, even if this awareness does not consistently translate into behavior. This awareness aligns with the observations by Bourgeus et al. (2024) and Prince et al. (2024), whose research indicates that users are indeed becoming more informed about their data privacy and are consequently starting to recognize the critical importance of understanding how data-collection processes affect them. This heightened attention to privacy policies, even if imperfectly executed, points toward an evolving and more conscious approach to data-sharing in the digital realm.

A similar finding is observed in Statement 9, which also garnered a positive mean score of 3.83 (SD=0.942). This response indicates that participants would be more willing to disclose personal information under stronger and more protective regulatory

frameworks, highlighting that caution toward data-sharing is conditional rather than absolute. This directly aligns with the study by Koul et al. (2025), which demonstrated that robust legal frameworks significantly improve consumers' confidence in utilizing digital platforms. This enhanced sense of security, driven by secured legal conditions, leads directly to an increased willingness among consumers to share their personal data.

The factor of trust also plays a pivotal role, as highlighted by Statement 10, which received a positive mean score of 3.63 (SD=0.987). This result reinforces a clear relationship between trust and data-sharing behavior, suggesting that platform trust functions as a prerequisite for data disclosure. As Treiblmaier and Chong (2007) established, users are significantly more inclined to share their data with a platform they trust, underscoring the importance of transparent and secure data governance practices in building and maintaining consumer confidence.

Conversely, the data reveals significant skepticism regarding data usage, particularly demonstrated by the neutral response to Statement 5, which recorded a mean score of 2.76 (SD=1.149). The relatively lower score on this inverse statement suggests that respondents do not fully trust platforms in their subsequent use of shared data. This outcome points to heightened privacy concerns among users, which aligns with the findings of Neves et al. (2024) that significant worries about data utilization are indicative of a pervasive and ongoing concern over privacy.

The convenience of online sharing is also viewed with neutrality, as shown by Statement 6, which received a neutral mean score of 3.09 (SD=1.069). This suggests that perceived convenience alone is insufficient to generate strong positive attitudes toward data-sharing, as persistent privacy concerns complicate the perceived ease of online disclosure. According to Azzopardi et al. (2025), while the technical ease of online sharing is undeniable, the associated security concerns and perceived risks are substantial enough to diminish the perceived effortlessness, leading to this non-committal, neutral evaluation.

Finally, the participants held a balanced perspective regarding the trade-off between risks and benefits, with Statement 7, yielding a mean score of 3.25 (SD=1.087). This result reflects a lack of consensus among respondents, indicating that while some believe the benefits outweigh the risks, a considerable portion remain unconvinced. This cautious assessment reinforces the broader pattern of skepticism surrounding data-sharing, as individuals are acutely aware of potential adverse consequences such as identity theft and the misuse of personal information, as also noted by Bourgeus et al. (2024).

Table 7 provides a detailed analysis of the respondents' attitudes toward data privacy concerns, and reveals a generally strong positive attitude overall, with an overall mean score of 3.96. The greatest level of concern is observed in Statement 6, which recorded a mean score of 4.12 (SD=0.884). This result suggests a high level of perceived risk when consumers encounter unfamiliar or newly established platforms. Such heightened concern suggests that unfamiliarity functions as a key risk trigger in digital environments. This finding aligns with the arguments of Solove (2004), who posits that users are inherently hesitant to share their information with platforms they do not know

well due to the potential for undisclosed or heightened risks. This hesitation reflects a fundamental safety mechanism applied to the digital sphere.

Table 7.
Descriptive Statistics for Attitude towards Data Privacy Concerns

Attitude Towards Data Privacy Concerns	Mean	SD	QD
1. Concern About Online Collection and Storage of Personal Information	3.86	0.894	Positive
2. Concern About Misuse of Shared Personal Data	3.92	0.837	Positive
3. Discomfort with Sharing Financial Information Online	4.01	0.852	Positive
4. Expectation of User Notification Regarding Data Usage	3.99	0.866	Positive
5. Doubt About Social Media Companies' Use of Shared Information	3.82	0.877	Positive
6. Perceived Risk of Sharing Data with Unknown or New Websites	4.12	0.884	Positive
7. Perception of Profit Priority Over User Data Safety	3.74	0.912	Positive
8. Concern About Lack of Transparency in Online Data Storage	3.95	0.874	Positive
9. Perceived Risk of Data Exposure to Hackers	4.12	0.902	Positive
10. Discomfort with Online Activity Tracking After Data Sharing	4.07	0.871	Positive

A similarly high level of concern is evident in Statement 9, which also obtained a mean score of 4.12 (SD=0.902). This strong agreement reflects a deep-seated fear of cyber threats, largely influenced by the high record of widely publicized data breaches in recent years. According to a report by the IBM Security (2020), the increasing frequency of data breaches and hacking incidents has significantly heightened user awareness regarding the vulnerabilities of personal data stored online. Importantly, this concern appears to stem less from doubts about platform intentions and more from perceived systemic weaknesses within the digital ecosystem.

In addition, respondents expressed significant anxiety related to financial data, as indicated by Statement 3, which secured a mean score of 4.01 (SD=0.852). This strong feeling of unease highlights that financial data is considered a highly sensitive category of personal information. As noted in a study by Woetzel et al. (2021), users are demonstrably more cautious about disclosing financial details due to the elevated risk of financial fraud and identity theft, thereby placing security considerations above convenience when monetary assets are involved.

Although the remaining three statements (Statements 1, 5, and 7) also indicate a positive attitude toward data privacy concerns, they ranked slightly lower than the statements emphasizing immediate risks such as hacking or financial loss. Statement 1 recorded a mean score of 3.86 (SD=0.894), suggesting that while respondents are generally aware and concerned about the collection and storage practices of platforms, their level of concern is less intense than that associated with financial or cybersecurity threats. Custers et al. (2020) suggest that concerns related to storage and data management are essential. However, perceived risks in this area often depends on a platform's transparency in handling user data and the clarity of its privacy regulations.

Similarly, Statement 5, demonstrated a positive attitude with a mean score of 3.82 (SD=0.877). This finding indicates that respondents recognize the potential misuse of their data by social media companies but do not perceive it as an immediate or severe threat. This interpretation aligns with Zuboff's (2019) conceptualization of the social media business model as "surveillance capitalism," where user-shared data is commodified for profit. The moderate score may reflect a degree of reluctant acceptance of this model, even as concerns remain present.

Finally, Statement 7 recorded the lowest positive mean score at 3.74 (SD=0.912). This result suggests that respondents are aware of the financial motivations driving online platforms to monetize user data, potentially at the expense of robust data protection measures. Uwayezu et al. (2025) noted that social media companies frequently prioritize profit through targeted advertising using user data, which contributes to public awareness of the privacy-profit trade-off. Nevertheless, the comparatively lower mean score implies that respondents may not perceive these practices as posing a direct or immediate threat to their personal data.

G. Subjective Norms toward Data-Sharing Behavior and Data Privacy Concerns of Digital Consumers

Table 8.
Descriptive Statistics for Subjective Norms

Construct	Mean	Std. Deviation	N
Subjective Norms Towards Data-Sharing Online	3.26	0.751	500
Subjective Norms Towards Data Privacy Concerns	3.82	0.595	500

The analysis of subjective norms toward online data-sharing, as presented in Table 8, indicates a mean score of 3.26 (SD=0.751). This value, situated close to the neutral midpoint of the scale, suggests that respondents generally do not experience a strong social pressure (or lack thereof) to share their personal data online. While studies such as Krasnova et al.'s (2009) confirm that social influence can affect a user's willingness to disclose information, the relatively modest score here implies that social norms do not act as a strong positive driver for data-sharing in this sample. Consequently, while some individuals may be influenced by peers or perceived group behavior, the decision to share personal data is largely viewed as a personal choice rather than one dictated by social expectation.

In contrast, the measure for Subjective Norms Towards Data Privacy Concerns yielded a substantially higher mean score of 3.82 (SD=0.595). This result clearly indicates that concern for privacy constitutes a more salient social norm and collective consideration among the respondents. Such a pattern reflects growing public awareness and a shared understanding of the risks associated with data-sharing, thereby fostering a social environment in which expressing privacy concerns is socially acceptable and increasingly normative. As supported by Marin et al. (2020), rising awareness of data-

sharing risks has led users to more readily express and reinforce strong privacy concerns within their social circles, particularly when navigating online environments where data is notably vulnerable.

This distinction is further emphasized by a direct comparison of the two mean scores, where subjective norms toward data privacy concerns (M = 3.82) are notably stronger than subjective norms toward online data-sharing (M = 3.26). The findings reveal a clear psychological priority, whereby respondents are more influenced by collective norms that emphasize privacy protection than by any social expectation to engage in data-sharing. Overall, this disparity highlights a community that is socially conscious of the importance of data protection and inclined to prioritize vigilance over conformity in matters related to personal data disclosure.

Table 9.

Descriptive Statistics for Subjective Norms towards Data-Sharing Online

Subjective Norms Towards Data-Sharing Online	Mean	SD	QD
1. Comfort with Sharing Personal Data Online	3.44	0.976	Neutral
2. Perceived Security of Data Shared with Reputable Companies	3.32	0.928	Neutral
3. Willingness to Share Data for Improved Online Experience	3.34	1.027	Neutral
4. Trust in Companies' Responsible Use of Personal Data	3.67	0.943	Positive
5. Lack of Concern About Online Data Use	3.25	1.067	Neutral
6. Convenience of Sharing Data Online	2.97	1.099	Neutral
7. Perceived Benefit–Risk Balance of Online Data Sharing	3.75	0.958	Positive
8. Attention to Privacy Policies Before Data Sharing	2.84	1.078	Neutral
9. Willingness to Share Data Under Stronger Privacy Regulations	2.88	1.086	Neutral
10. Likelihood of Sharing Data with Trusted Online Platforms	3.17	1.11	Neutral

Table 9 provides the descriptive statistics for Subjective Norms Towards Data-Sharing Online, indicating an overall neutral-to-moderate level of social pressure. However, certain aspects of perceived prevalence scored higher. For instance, Statement 4 yielded a relatively positive mean score of 3.67 (SD = 0.943). This suggests that respondents perceive data-sharing as a common or normalized behavior within their immediate social circles, thereby establishing a relatively positive subjective norm. As noted by Krasnova et al. (2009), when individuals view data-sharing as a prevalent practice among their acquaintances, they are generally more inclined to engage in similar behaviors. Ziller et al. (2025) further highlight the key role of local social influence in promoting data-sharing when it is observed within one's personal network.

Similarly, the overall acknowledgment of data-sharing's prevalence is strong, as indicated by Statement 10, which scored a mean of 3.75 (SD = 0.958). This is the highest score in this category, reflecting respondents' clear recognition of the widespread nature of data-sharing in contemporary digital society. Research by Binns (2018) and Marin et al. (2022) supports this perception, attributing the normalization of data-sharing practices to the rapid expansion and integration of the digital economy into daily life.

Focusing on the immediate peer group, Statement 1 remained near the midpoint, with a mean score of 3.44 (SD = 0.976). This result suggests that while respondents generally perceive their peers as viewing data-sharing as normal or acceptable, the score is not high enough to suggest significant social pressure. Studies such as Chi et al. (2012) consistently show that peer behavior influences the propensity to share data online. As suggested by Ziller et al. (2025), while peer attitudes influence willingness to share, the moderate mean score here implies a norm of acceptance rather than coercive social compliance.

In contrast, the influence of public figures on data-sharing behavior is minimal. Statement 8 received the lowest mean score in this category at 2.84 (SD = 1.078). This score, which leans toward disagreement, suggests that celebrity data-sharing behaviors do not significantly influence respondents' own disclosure decisions. This finding is consistent with Ziller et al. (2025) research, which noted that while celebrities may influence consumer choices in areas such as fashion, their impact is markedly weaker in privacy-related decisions such as online data-sharing.

Reinforcing the low level of direct social pressure, Statement 9 also remained near the midpoint, with a mean score of 2.88 (SD = 1.086). This neutral response suggests that awareness of others' data-sharing behavior does not translate into a motivating factor for respondents' own actions. The low mean score implies that respondents do not feel a strong sense of social obligation to share data due to conformity. Krasnova et al. (2009) argue that personal privacy concerns often override external social influence in decisions about data disclosure.

Finally, the influence of social media figures is limited, as shown by Statement 6, which recorded a low mean score of 2.97 (SD = 1.099). Despite the recognized influence of social media figures in other domains, this result indicates only minimal impact on privacy-related decisions. Marwick (2023) suggests that followers may resist influencer behavior when issues involve privacy-sensitive matters. This further confirms that data-sharing remains primarily an individual decision, relatively resistant to external social pressures than other consumer behaviors.

Table 10.

Descriptive Statistics for Subjective Norms towards Data Privacy Concerns

	Subjective Norms Towards Data Privacy Concerns	Mean	SD	QD
1.	Friends' Concern About Online Data Sharing	3.75	0.794	Positive
2.	Discussion of Data Privacy Concerns Among Peers	3.53	0.922	Positive
3.	Peer Discouragement from Sharing Data on Unsecured Platforms	3.77	0.941	Positive
4.	Influence of Media Reports on Data Breaches and Privacy Issues	3.7	0.859	Positive
5.	Family Advice on Cautious Online Data Sharing	4.11	0.837	Positive
6.	Impact of Data Protection Advertisements on Risk Awareness	4.01	0.856	Positive
7.	Perceived Cautiousness of Social Circle Toward Data Sharing	3.84	0.836	Positive
8.	Social Norms Supporting Online Data Protection	4.03	0.819	Positive
9.	Friends' Belief in Companies' Inadequate Data Security	3.57	0.878	Positive
10.	Perceived Privacy Concern Among People Known Personally	3.9	0.872	Positive

Table 10 illustrates the specific components of Subjective Norms Towards Data Privacy Concerns, which overall demonstrated a strong positive mean level. The highest influence came from Statement 5, which received a high mean score of 4.11 (SD = 0.837). This result indicates the strong influence of family in shaping an individual's cautious orientation toward online data privacy. This positive subjective norm suggests that family members serve as a key source of early guidance, instilling heightened awareness and caution. This aligns with the findings of Bélanger and Crossler (2011), who emphasized that close social groups, particularly families, are significant sources of privacy-related advice, with parental guidance being especially effective in shaping protective data-related behaviors**.**

The perception of privacy as a collective societal value also scored highly, with Statement 8 yielding a mean score of 4.03 (SD = 0.819). This result reinforces the idea that broader social expectations and norms act as a powerful external motivator for prioritizing data privacy. The finding is consistent with Wang (2019), who noted that when individuals perceive privacy protection as an expected societal norm, they are significantly more likely to adopt online behaviors that reflect this priority. This high score suggests that data protection has shifted from an individual concern to a widely recognized and socially endorsed imperative.

Furthermore, external media influence plays a substantial role, with Statement 6 recording a strong mean score of 4.01 (SD = 0.856). This highlights the significant impact of advertisements and public campaigns in raising awareness of data privacy risks. As noted by Ara et al. (2022), public awareness campaigns on data protection are instrumental in shaping individuals' understanding of the vulnerabilities associated with sharing personal information online. These media efforts effectively increase risk awareness, thereby encouraging more vigilant and cautious behavior regarding online data sharing. Overall, these findings suggest that family, social expectations, and media exposure collectively contribute to an environment that promotes strong privacy awareness.

However, the influence of peers regarding organizational trust is less pronounced. Statement 9 recorded a mean score of 3.57 (SD = 0.878), falling near the midpoint. While friends' concern is generally positive, the moderate score suggests that respondents are not strongly influenced by peers' specific views on how companies manage personal data. As theorized by Pavlou (2003), trust in organizations is largely a matter of individual evaluation in data-sharing contexts. Accordingly, the mean score indicates that while peers may express concern, these views do not substantially override respondents' own judgments.

Similarly, the frequency of privacy-related discussion among peers is moderate, as Statement 7 yielded a mean score of 3.53 (SD = 0.920). This suggests that while privacy concerns are present within social circles, they are not a pervasive or dominant topic of discussion. Kim and Elias (2015) observed that even individuals with high privacy concern may find that their broader social environment does not fully reflect their level of engagement.

Finally, perceptions of widespread peer concern are moderate, with Statement 10 achieving a mean score of 3.90 (SD = 0.872). Although this score remains positive, it is lower than those associated with family or societal influence. This implies some uncertainty among respondents regarding the extent to which others in their immediate social groups share similarly high levels of concern. As Rader (2023) suggests, despite the growing importance of data privacy, individuals may underestimate others' concern, particularly when the convenience of online services is highly salient**.**

H. Perceived Behavioral Control toward Data-Sharing Behavior and Data Privacy Concerns of Digital Consumers in Cauayan City, Isabela

Table 11 summarizes the average scores for Perceived Behavioral Control (PBC) across two distinct areas, i.e., data-sharing behavior and data privacy concerns. The results indicate that digital consumers possess a generally strong sense of control in both domains.

Table 11.
Descriptive Statistics for Perceived Behavioral Control

Construct	Mean	Std. Deviation	N
Perceived Behavioral Control Towards Data-Sharing Behavior	3.84	0.642	500
Perceived Behavioral Control Towards Data Privacy Concerns	3.73	0.667	500

The mean score for Perceived Behavioral Control related to data-sharing behavior is 3.84 (SD = 0.642). This relatively high score indicates that the majority of participants feel confident and capable of exercising personal agency when deciding whether and how to share their personal information. This sense of internal control is a crucial predictor of behavior, supporting the perspective of Akdeniz et al. (2023) that individuals who perceive greater control are more likely to willingly engage in data-sharing. Furthermore, as Zenk-Möltgen et al. (2018) explain, perceived control encompasses both belief in one's ability to perform an action (self-efficacy) and the subjective perception of freedom in making that choice.

The mean score for Perceived Behavioral Control related to data privacy concerns is slightly lower at 3.73 (SD = 0.667), yet still suggests that participants feel they have a considerable degree of influence over protecting their personal information. This indicates that consumers believe they can actively take steps to mitigate privacy risks. According to Biber et al. (2024), a stronger sense of perceived behavioral control is directly linked to a greater likelihood of adopting privacy-protective behaviors, such as adjusting privacy settings, selectively limiting shared data, or actively using privacy-enhancing tools. Similarly, Ho et al. (2022) highlight that perceived behavioral control is a powerful determinant, alongside attitudes and social influences, in shaping how individuals, particularly young people, actively manage their online privacy.

Crucially, comparison of the two mean scores reveals a subtle but meaningful distinction: digital consumers perceive more control over their own data-sharing actions

(3.84) than over maintaining their privacy (3.73). This modest disparity suggests that while individuals feel confident in making personal decisions to click "Share" or "Do Not Share," they recognize that achieving comprehensive privacy protection often involves external constraints that are more difficult to manage. These factors include the complexity and lack of transparency of platform privacy settings, as well as organizational practices related to data collection and storage, which may limit the perceived effectiveness of individual protective efforts.

Table 12 provides detailed descriptive statistics for respondents' Perceived Behavioral Control (PBC) towards data-sharing online, confirming an overall positive level of perceived control. This suggests that consumers generally believe they possess the capability and resources to manage their data-related actions.

The strongest sense of control is demonstrated in Statement 2, which scored the highest mean of 4.12 (SD = 0.847). This high score indicates that digital consumers are aware of privacy risks and actively regulate the volume of personal information they disclose. This self-restrictive behavior represents a direct manifestation of PBC and aligns with the findings of Hsu et al. (2022), who found that individuals with heightened privacy concerns are generally less willing to share personal information, prioritizing caution through self-limitation.

Table 12.
Descriptive Statistics for Perceived Behavioral Control towards Data-Sharing Online

Perceived Behavioral Control Towards Data-Sharing	Mean	SD	QD
1. Confidence in Controlling Shared Online Data	3.71	0.952	Positive
2. Self-Limitation of Personal Information Shared Online	4.12	0.847	Positive
3. Ability to Stop Sharing Data Online	3.94	0.886	Positive
4. Knowledge of Protecting Personal Data Against Online Threats	3.99	0.83	Positive
5. Perceived Control Over Data After Online Sharing	3.71	0.908	Positive
6. Awareness of Tools to Limit Online Data Sharing	3.84	0.887	Positive
7. Ease of Managing Online Privacy Settings	3.68	0.869	Positive
8. Perceived Platform Support for Data Access and Control	3.67	0.872	Positive
9. Capability to Make Informed Data-Sharing Decisions	3.79	0.887	Positive
10. Ability to Avoid Online Data Sharing When Desired	3.95	0.905	Positive

Confidence in digital literacy also scored highly, with Statement 4, receiving a mean score of 3.99 (SD = 0.83). This indicates that respondents believe they possess adequate digital skills and knowledge to effectively safeguard their data. This belief in self-efficacy is a core component of PBC. Büchi et al. (2017) support this interpretation, finding that individuals who perceive themselves as knowledgeable about online data protection are significantly more likely to engage in proactive privacy-protective behaviors.

Furthermore, respondents expressed a strong belief in their fundamental freedom of choice, as reflected in Statement 10, which recorded a mean score of 3.95 (SD = 0.905). This result reveals a strong sense of volitional control over the initiation of data-sharing.

As Hajli and Lin (2016) demonstrated, users' perceived control over their information significantly influences their willingness to share data on social networking sites, as higher perceived control reduces perceived privacy risks and fosters more positive attitudes toward sharing.

Despite the generally high scores, two statements reflecting control over platform practices and post-sharing data recorded the lowest means, indicating key areas of vulnerability**.** Statement 8 recorded the lowest mean score at 3.67 (SD = 0.872). This suggests that while respondents are confident in their own actions, they remain skeptical about the level of control platforms provide over personal information. The lower score reflects a perceived limitation in platform-based data control, contributing to consumer skepticism. This finding aligns with Benson et al. (2015), who found that users often lack awareness of how their information is used by platforms and third parties, leading to doubts about the practical extent of control they truly possess.

The perceived difficulty of managing privacy settings further constrained PBC, as Statement 7 recorded the second-lowest mean score of 3.68 (SD = 0.869). This implies that although digital consumers recognize the importance of adjusting privacy settings, the process is often perceived as complex or time-intensive, acting as a practical barrier to regular engagement. Craig (2025) noted that managing privacy settings can be cognitively demanding, reinforcing perceptions that the task is overwhelming and discouraging frequent adjustment.

Finally, two statements recorded the same mean score of 3.71, jointly occupying the lower range and highlighting a notable shift in perceived control. Statement 1 (SD = 0.952) and Statement 5 (SD = 0.908) suggest that while users may feel a degree of control prior to sharing data, this sense of control diminishes once the data has been disclosed. As Shulman and Meyer (2022) explained, individuals often experience strong perceived control over initial disclosure decisions, but this perception weakens substantially after sharing, as users recognize their limited authority over subsequent data use or dissemination, which can result in heightened anxiety and regret.

Table 13.

Descriptive Statistics for Perceived Behavioral Control towards Data Privacy Concerns

Perceived Behavioral Control Towards Data Privacy Concerns	Mean	SD	QD
1. Confidence in Identifying Privacy-Focused Online Platforms	3.88	0.838	Positive
2. Control Over Personal Information to Reduce Privacy Risks	3.85	0.833	Positive
3. Regular Updating of Online Privacy Settings	3.75	0.917	Positive
4. Perceived Ability to Prevent Unauthorized Data Access	3.8	0.867	Positive
5. Confidence in Detecting Phishing or Fraudulent Platforms	3.59	0.923	Positive
6. Knowledge of Tools for Enhancing Data Privacy Protection	3.65	0.901	Positive
7. Awareness of Irregular or Harmful Data-Related Activities	3.7	0.893	Positive
8. Knowledge of Reporting Data Misuse or Breaches	3.66	0.868	Positive
9. Understanding of Data-Sharing Terms and Conditions	3.84	0.879	Positive
10. Perceived Ability to Prevent Misuse of Shared Data by Companies	3.61	0.927	Positive

Table 13 summarizes the descriptive statistics for respondents' perceived behavioral control towards data privacy concerns, indicating a generally positive level of perceived control among digital consumers.

The highest scores reflect strong confidence in identifying trustworthy platforms and managing shared information. For example, Statement 1 achieved a mean score of 3.88 (SD = 0.838), suggesting that digital consumers are confident in their ability to recognize trustworthy online platforms. This finding aligns with Bélanger and Crossler (2011), whose study revealed that consumers often rely on privacy seals and third-party verification programs as indicators of trustworthiness, thereby contributing to a moderate level of confidence in platform recognition.

Further reinforcing this sense of control, Statement 2 received a mean score of 3.85 (SD = 0.833). This result indicates that digital consumers believe they are capable of performing behaviors necessary to effectively reduce privacy risks. This belief in personal agency is consistent with the findings of Atalay and Yücel (2024), who suggest that individuals who feel control over their personal information are more likely to believe they can manage privacy risks effectively. This enhanced sense of control is essential, as it often translates into greater confidence when making data-sharing decisions.

In addition, a high level of confidence was expressed regarding comprehension of legal language, with Statement 9 yielding a mean score of 3.84 (SD = 0.879). This response suggests that respondents feel confident in their ability to interpret the complex language used in privacy agreements and consent forms. According to Park (2013), this perceived confidence in understanding data-sharing terms may positively influence users' willingness to share personal data, as they feel equipped to navigate privacy agreements more effectively.

While the overall trend for perceived behavioral control is positive, Statement 5 recorded the lowest mean score among all items at 3.59 (SD = 0.923). This relatively lower score reflects notable uncertainty among digital consumers, indicating that they recognize the increasing sophistication of online scams and deceptive tactics, thereby reducing confidence in accurately identifying threats. This result supports Wang et al. (2016), who argued that although individuals may express confidence in detecting phishing attempts, this confidence is frequently challenged by the complexity of modern scams, highlighting a potential gap between self-assessed confidence and actual detection ability.

Concern regarding post-sharing data control is evident in Statement 10, which received the second-lowest mean score of 3.61 (SD = 0.927). Although still positive, this score suggests that respondents have limited confidence in their ability to control how companies ultimately use their data once it has been shared. This aligns with Durnell et al. (2020), who found that individuals often express skepticism about their ability to prevent corporations from misusing shared personal data. This perceived lack of ultimate control contributes to broader privacy concerns and may intensify distrust toward organizations that handle personal information.

Furthermore, Statement 6 received a mean score of 3.65 (SD = 0.901), indicating a moderate but positive level of perceived behavioral control. This implies that digital consumers are generally aware of the availability of privacy-enhancing tools. However, the moderate score suggests that while basic awareness exists, it does not necessarily translate into confident or effective application. Trepte (2021) highlighted this issue, noting that many users overestimate their ability to select and use effective privacy technologies, which can result in inadequate protection and a false sense of security. Accordingly, the observed confidence level may reflect surface-level familiarity rather than deep, functional understanding of privacy-enhancing measures.

I. Behavioral Intention toward Data-Sharing Behavior and Data Privacy Concerns of Digital Consumers

Results of the study show a relatively high level of intention (M = 3.54; SD = 0.706) among respondents towards data-sharing. This suggests that respondents are more likely to share their information online when there is an assurance of safe data usage, trust, and convenience. According to Aragon et al. (2024), transparency significantly influences users' willingness to share their data, particularly in relation to how their data is handled and used, and how they perceive data privacy.

Table 14.
Descriptive Statistics for Intention

	Intention	Mean	SD	QD
1.	Likelihood of Future Online Data Sharing	3.27	0.932	Neither
2.	Intention to Share Data for Enhanced Online Experience	3.51	0.963	High
3.	Willingness to Share Data for Personalized Services	3.63	0.872	High
4.	Intention to Share Data with Trusted Websites or Apps	3.63	0.95	High
5.	Openness to Data Sharing When Benefits Are Provided	3.53	0.898	High
6.	Likelihood of Data Sharing Under Perceived Safety	3.66	0.958	High
7.	Intention to Share Personal Information for Better Service Access	3.62	0.888	High
8.	Likelihood of Data Sharing Based on Trusted Company Recommendation	3.66	0.876	High
9.	Likelihood of Data Sharing for Access to New Online Services	3.44	0.869	Neither
10.	Intention to Increase Online Data Sharing for Greater Benefits	3.44	0.957	Neither

Table 14 presents the descriptive statistics for data-sharing intention, revealing a generally high willingness to share data under specific conditions that emphasize user safety and convenience. Respondents expressed the strongest intention to share personal information when they felt safe in doing so (M = 3.66, SD = 0.958), when online platforms were recommended by trusted companies (M = 3.66, SD = 0.876), and when platforms offered personalized services (M = 3.63, SD = 0.950). The consistently high mean scores across these items suggest that digital consumers are highly motivated to engage in data-sharing when they perceive a strong sense of safety, trust, and personalized convenience.

This finding supports the work of Bourgeus et al. (2024), who emphasized that user empowerment and control over shared data significantly enhance willingness to participate in online data-sharing activities.

Despite this high conditional intention, the mean scores for generalized and future-oriented sharing intentions were comparatively lower, indicating a degree of caution. Responses were only moderate to slightly high when asked about sharing data in the future (M = 3.27, SD = 0.932), signing up for new websites (M = 3.44, SD = 0.869), and sharing data in the future in exchange for additional benefits (M = 3.44, SD = 0.957). These slightly lower scores, closer to the scale's midpoint, suggest that while security, trust, and convenience are strong motivators for immediate data-sharing, they do not fully eliminate underlying hesitation regarding broader or future disclosure. This pattern implies that perceived risks related to privacy violations and information misuse continue to moderate overall, unconditional intentions to share data online.

J. Predictors of Data-Sharing Intention

A linear regression analysis was performed in order to determine whether the attitudes, subjective norms, and perceived behavioral control in terms of data sharing online and data privacy concerns of digital consumers in the City of Cauayan were significant predictors of their intention to share personal information online. It must be noted that 47.9% of the variation in intention was explained by the variation in attitude, subjective norms, and perceived behavioral intention. The analysis presented in Table 15 showed that the model is significant. Additionally, attitudes ($t = 8.225$, $p < 0.01$), subjective norms ($t = 7.169$, $p < 0.01$), and perceive behavioral control towards data sharing online ($t = 7.169$, $p < 0.01$), $p < 0.01$) are significant predictors, showing that for every one unit increase in attitude, subjective norms, and perceive behavioral control towards data sharing online, behavioral intention is increased by 0.367, 0.274 and 0. 0.254, respectively.

Table 15.
Linear Regression Model of Data-Sharing Intention and the Predictor Variables

Predictor	Estimate	SE	t	p
Intercept	0.38	0.20	1.93	0.05
Attitude towards data sharing online	0.37	0.05	8.23	< .001*
Attitude towards data privacy concerns	0.07	0.04	1.62	0.11
Subjective norms towards data-sharing online	0.27	0.04	7.17	< .001*
Subjective norm towards data privacy concerns	-0.06	0.06	-1.15	0.25
Perceived behavioral control towards data sharing online	0.26	0.06	4.32	< .001*
Perceived behavioral control towards data privacy concerns	-0.01	0.05	-0.24	0.81

*Significant at α= 0.01

This study tested two sets of hypotheses to examine whether components of the Theory of Planned Behavior, namely attitude, subjective norms, and perceived

behavioral control, predict participants' intention to share personal data online in relation to data sharing practices and data privacy concerns.

The first hypothesis examined whether participants' attitude, subjective norms, and perceived behavioral control toward data sharing online significantly predict their intention to share personal data. The null hypothesis (H01) stated that these factors would not significantly predict intention, while the alternative hypothesis (Ha1) proposed a significant predictive relationship. The findings led to the rejection of H01 and the acceptance of Ha1, indicating that attitude, subjective norms, and perceived behavioral control toward data sharing online significantly predict participants' intention to share personal data.

This result confirms that the three components of the Theory of Planned Behavior are influential and statistically significant determinants of data-sharing intention. The finding is consistent with existing literature. Pavlou (2003) emphasized that a positive attitude toward an online platform plays a critical role in users' decision-making processes. Similarly, Culnan and Armstrong (1999) highlighted that trust increases individuals' willingness to share personal information. The influence of subjective norms aligns with Kim and Elias (2015), who found that individuals are more likely to disclose personal information when they observe such behavior within their social networks. In addition, the significance of perceived behavioral control supports the findings of Bélanger and Crossler (2011), who reported that individuals who perceive greater control over their personal data are more willing to share information online.

The second hypothesis assessed whether participants' attitude, subjective norms, and perceived behavioral control toward data privacy concerns predict their intention to share personal data online. The null hypothesis (H02) proposed that these factors would not significantly predict intention, while the alternative hypothesis (Ha2) suggested a significant predictive effect. The results supported the acceptance of H02 and the rejection of Ha2, indicating that these TPB components related to data privacy concerns do not significantly predict participants' intention to share personal data online.

This finding suggests that although participants may be aware of and concerned about data privacy, these concerns do not play a decisive role in shaping their intention to share personal information in this context. Instead, the results point to the presence of a privacy paradox, wherein privacy concerns exist but do not translate into behavior. Schmeling et al. (2025) similarly observed that perceived benefits, convenience, and functionality of online platforms often outweigh privacy concerns in users' decision-making processes. Chi et al. (2012) and Büchi et al. (2022) further noted that even when individuals express high levels of privacy concern, subjective norms and social influence can exert a stronger effect on data-sharing behavior. Consistent with these findings, Oesterreich et al. (2025) concluded that privacy concerns are not always the primary predictors of data-sharing intention, particularly when immediate benefits and convenience dominate users' evaluations.

IV. CONCLUSION AND IMPLICATIONS

This study successfully analyzed the data-sharing behavior and privacy concerns of digital consumers in Cauayan City, Isabela, a distinct local context within the Philippines that is often overlooked in national privacy research. By applying descriptive statistics and regression analysis to the core tenets of the Theory of Planned Behavior (TPB) namely attitude, subjective norms, and perceived behavioral control**,** this research provided comprehensive insights into local data practices and intentions.

The principal finding indicates that consumers demonstrate a higher sense of attitude, subjective norms, and perceived behavioral control toward data sharing online than toward data privacy concerns. The higher mean scores for the TPB constructs related to sharing demonstrate that users' intentions are primarily driven by the perceived convenience, trust, and practical benefits offered by online platforms. Essentially, online data sharing is viewed through a pragmatic lens, where immediate utility and ease of use overshadow more abstract privacy risks.

A critical and counterintuitive finding was the non-significant predictive power of attitude, subjective norms, and perceived behavioral control related to data privacy concerns on data-sharing intention. This supports the notion that despite frequent global and national reports of data breaches and identity theft, privacy concerns do not serve as the primary deterrent to data sharing for this consumer group.

This result underscores the presence of a "privacy paradox," suggesting that the immediate and tangible rewards and convenience of online services effectively outweigh the perceived long-term and abstract risks associated with data sharing. The decision to share data is thus less about the fear of privacy violations and more about maximizing platform use.

This study provides compelling evidence for policymakers and legal scholars. It emphasizes that since consumer intention is not adequately safeguarded by personal privacy concerns alone, external regulatory mechanisms must be strengthened. The findings highlight the urgency of reviewing and reinforcing the existing Philippine Data Privacy Act (DPA) or implementing new regulations that place greater emphasis on transparency, accountability, and redress mechanisms for data misuse, even when consumers willingly share their data. This is particularly salient given the prevalence of data breaches and identity theft in the national context.

While robust, the study has certain limitations. First, the reliance on a self-reported quantitative survey introduces the potential for social desirability bias, wherein participants may overstate their confidence in managing privacy, particularly perceived behavioral control, or their adherence to social norms, thus potentially inflating scores related to data-sharing intention. Second, the study's scope was geographically limited to Cauayan City, Isabela, which restricts the direct generalizability of the findings to the broader population of Filipino digital consumers. Consumers in highly urbanized centers such as Metro Manila or Cebu, who experience different levels of digital exposure and technological access, may exhibit different data-sharing behaviors.

To address these limitations and expand on the findings, future research should consider employing a mixed-methods approach by supplementing quantitative surveys with qualitative interviews or focus group discussions to gain a deeper and less biased

understanding of the motivations underlying the privacy paradox. Future studies should also replicate this research across various urban and rural locations in the Philippines to compare behavioral control and data-sharing intentions across diverse socioeconomic and technological environments.

This study, however, successfully illustrates the attitudes, subjective norms, and perceived behavioral control of digital consumers in Cauayan City, Isabela. The emphasis on these key influential factors highlights the intentions of respondents with respect to their data privacy.

V. DISCLOSURE STATEMENT

The author declares no conflict of interest.

VI. REFERENCES

Akdeniz, E., Borschewski, K. E., Breuer, J., & Voronin, Y. (2023). Sharing social media data: The role of past experiences, attitudes, norms, and perceived behavioral control. *Frontiers in big data, 5*, 971974. https://doi.org/10.3389/fdata.2022.971974

Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. *Journal of Retailing and Consumer Services, 68*, 103042. https://doi.org/10.1016/j.jretconser.2022.103042

Ara, A., Zainol, Z., & Duraisamy, B. (2022). The effects of privacy awareness, security concerns and trust on information sharing in social media among public university students in Selangor. *International Business Education Journal, 15*(2), 93–110. https://doi.org/10.37134/ibej.Vol15.2.8.2022

Aragon, K. A. P., Cabudoc, M. A. L., Remolin, A. B., & Zamora, Z. M. D. (2024). Analyzing the impact of privacy concerns on consumer behavior. *International Journal of Research and Innovation in Social Science, 8*(12), 920–934. https://doi.org/10.47772/IJRISS.2024.8120077

Atalay, H. N., & Yücel, Ş. (2024). Decoding privacy concerns: the role of perceived risk and benefits in personal health data disclosure. *Archives of public health = Archives belges de sante publique, 82*(1), 180. https://doi.org/10.1186/s13690-024-01416-z

Auxier, B., & Anderson, M. (2021, April 7). *Social media use in 2021.* Pew Research Center. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Azizan, A., Abu Bakar, Z., Abdul Rahman, N., & Masrom, S. (2018). A comparative evaluation of search engines on finding specific domain information on the web. *International Journal of Engineering & Technology, 7*(4), 1–4. https://doi.org/10.14419/ijet.v7i4.33.23471

Azzopardi, L., Nicol, E., Briggs, J., & Moncur, W. (2025, March). *Assessing risks in online information sharing*. In *Proceedings of the ACM SIGIR Conference on Human Information Interaction and Retrieval* (CHIIR). https://doi.org/10.1145/3698204.3716447

Bacay, I., Ramirez, R. A., Ramos, F. N., & Grimaldo, J. R. (2022). Factors influencing Shopee users' intention to purchase products during Shopee Philippines' big online shopping events. *Journal of Business and Management Studies, 4*(2), 27–37. https://doi.org/10.32996/jbms.2022.4.2.3

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). https://doi.org/10.5210/fm.v11i9.1394

Bélanger, N., & Crossler, N. (2011). Privacy in the Digital Age: a Review of Information Privacy Research in Information Systems1. *MIS Quarterly*, *35*(4), 1017-A36. https://doi.org/10.2307/41409971

Belmonte, Z. J. A., Prasetyo, Y. T., Cahigas, M. M., Nadlifatin, R., & Gumasing, M. J. J. (2024). Factors influencing the intention to use e-wallet among generation Z and millennials in the Philippines: An extended technology acceptance model (TAM) approach. *Acta Psychologica, 250*, 104526. https://doi.org/10.1016/j.actpsy.2024.104526

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users. *Information Technology and People*, *28*(3), 426–441. https://doi.org/10.1108/itp-10-2014-0232

Bhandari, P. (2020). *Descriptive Statistics | Definitions, Types, Examples*. Scribbr. https://www.scribbr.com/statistics/descriptive-statistics/

Biber, M., Louis, W. R., & Smith, J. R. (2024). Predicting online privacy protection for Facebook users with an extended theory of planned behavior. *The Journal of Social Psychology, 165*(3), 313–332. https://doi.org/10.1080/00224545.2024.2319177

Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of Machine Learning Research, 81*, 1–11. https://proceedings.mlr.press/v81/binns18a.html

Bourgeus, A., Vandercruysse, L., & Verhulst, N. (2024). Understanding contextual expectations for sharing wearables' data: Insights from a vignette study. *Computers in Human Behavior Reports, 15*, 100443. https://doi.org/10.1016/j.chbr.2024.100443

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society, 9*(1). https://doi.org/10.1177/20539517211065368

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of internet skills for online privacy protection. *Information, Communication & Society, 20*(8), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Chi, H., Hueryren, Y., & Wei-chien, H. (2012). The moderating effect of subjective norm on cloud computing users' perceived risk and usage intention. *International Journal of Marketing Studies, 4*(6), 95. https://doi.org/10.5539/ijms.v4n6p95

Craig, M. J. A. (2025). Human–machine communication privacy management, privacy fatigue, and the conditional effects of algorithm awareness on privacy co-ownership in the social media context. *Computers in Human Behavior, 173*, 108786. https://doi.org/10.1016/j.chb.2025.108786

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1). https://doi.org/10.1287/orsc.10.1.104

Custers, B., et al. (2020). *EU Personal Data Protection in Policy and Practice*. T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-282-8

Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: Construction and validation of the concerns with the protection of informational privacy scale. *International Journal of Human–Computer Interaction, 36*(3), 1–15. https://doi.org/10.1080/10447318.2020.1794626

Gonzales, A. L. (2024, August 21). *Filipinos hope to grow income but worry about household finances*. Philippine News Agency. https://www.pna.gov.ph/articles/1231668

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics, 133*, 111–123. https://doi.org/10.1007/s10551-014-2346-x

Ho, S. S., Goh, T. J., & Chuah, A. S. F. (2022). Perceived behavioral control as a moderator: Scientists' attitude, norms, and willingness to engage the public. *PLOS ONE, 17*(10), e0275643. https://doi.org/10.1371/journal.pone.0275643

Hsu, C., Liao, Y., Lee, C., & Chan, L. K. (2022). Privacy Concerns and Information Sharing: The perspective of the U-Shaped Curve. *Frontiers in Psychology*, *13*, 771278. https://doi.org/10.3389/fpsyg.2022.771278

IBM Security. (2020). *Cost of a Data Breach Report 2020*.

Kim, J., Lee, C., & Elias, T. (2015). Factors affecting information sharing in social networking sites amongst university students. *Online Information Review*, *39*(3), 290–309. https://doi.org/10.1108/oir-01-2015-0022

Komnenic, M. (2025). *What Is Data Privacy? Complete Guide for Businesses*. https://termly.io/resources/articles/what-is-data-privacy/#what-is-data-privac

Koul, S., Verma, R., & Ajaygopal, K. V. (2025). Stakeholders' understanding of data privacy: Implications for digital credit consumer. *Cogent Business & Management, 12*(1). https://doi.org/10.1080/23311975.2025.2568200

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society, 2*, 39–63. https://doi.org/10.1007/s12394-009-0019-1

Magadia, C. (2025, October 8). *YouTube strengthens lead as new TV*. Philippine Tribune. https://tribune.net.ph/2025/10/08/youtube-strengthens-lead-as-new-tv

Marín, V. I., Carpenter, J. P., & Tur, G. (2020). Pre-service teachers' perceptions of social media data privacy policies. *British Journal of Educational Technology*, *52*(2), 519–535. https://doi.org/10.1111/bjet.13035

Marín, V. I., Carpenter, J. P., Tur, G., & Williamson-Leadley, S. (2022). Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers. *Journal of Computers in Education*, *10*(4), 769–795. https://doi.org/10.1007/s40692-022-00243-x

Marwick, A. E. (2023). *The Private Is Political: Networked Privacy and Social Media.* Yale University Press. https://doi.org/10.12987/9780300271652

Mateo, J. (2024, September 19). *More Pinoys prefer YouTube for information, entertainment.* Philippine Star. https://www.philstar.com/headlines/2024/09/19/2386362/more-pinoys-prefer-youtube-information-entertainment

McBurney, D. H., & White, T. L. (2009). *Research methods (8th ed.).* Cengage Learning.

Neves, J., Turel, O., & Oliveira, T. (2024). Privacy concerns in social media use: A fear appeal intervention. *International Journal of Information Management Data Insights, 4*(2), 100260. https://doi.org/10.1016/j.jjimei.2024.100260

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Oesterreich, T. D., Anton, E., Hettler, F. M., et al. (2025). What drives individuals' trusting intention in digital platforms? An exploratory meta-analysis. *Management Review Quarterly, 75*, 3615–3667. https://doi.org/10.1007/s11301-024-00477-2

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

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, *7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Prince, C., Omrani, N., & Schiavone, F. (2024). Online privacy literacy and users' information privacy empowerment: The case of GDPR in Europe. *Information Technology & People, 37*(8), 1–24. https://doi.org/10.1108/ITP-05-2023-0467

Rader, E. (2023, August). Data privacy and pluralistic ignorance. In *Proceedings of the Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)* (pp. 457–471). USENIX Association. https://www.usenix.org/conference/soups2023/presentation/rader

Samaniego, A. (2023, September 22). *PhilHealth paralyzed by Medusa ransomware attack*. Manila Bulletin. https://mb.com.ph/2023/9/21/phil-health-paralyzed-by-medusa-ransomware-attack

Schmeling, J., al Dakruni, S., & Mergel, I. (2025). Data collaboration in digital government research: A literature review and research agenda. *Government Information Quarterly, 42*(3), 102063. https://doi.org/10.1016/j.giq.2025.102063

Shulman, Y., & Meyer, J. (2022). Degrees of perceived control over personal information: Effects of information relevance and levels of processing. *IEEE Access, 10*, 40596–40608. https://doi.org/10.1109/ACCESS.2022.3167025

Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age* (Vol. 1). NYU Press.

Spanaki, K., Karafili, E., & Despoudi, S. (2021). AI applications of data sharing in agriculture 4.0: A framework for role-based data access control. *International*

Journal of Information Management, 59, 102350. https://doi.org/10.1016/j.ijinfomgt.2021.102350

Stallings, W. (2020). Handling of personal information and deidentified, aggregated, and pseudonymized information under the California Consumer Privacy Act. *IEEE Security & Privacy*, *18*(1), 61–64. https://doi.org/10.1109/msec.2019.2953324

Tobin, D. (2024). *What is Data Privacy – and Why Is It Important?* Integrate.io. https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/

Treiblmaier, H., & Chong, S. (2007). Antecedents of the intention to disclose personal information on the Internet: A review and model extension. In *SIGHCI 2007 Proceedings* (Article 19). https://aisel.aisnet.org/sighci2007/19

Trepte, S. (2021). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory, 31*(4), 549–570. https://doi.org/10.1093/ct/qtz035

Uwayezu, E., Tenney, D., & McAdams, A. (2025). Evaluating social media user trade-off between free platform use and privacy concerns of AI-powered targeted advertising. *Journal of Business and Economic Studies, 2*(3), 1–10. https://doi.org/10.61440/JBES.2025.v2.65

Wang, D. (2019). A study of determinants of teenagers' privacy protection intentions on social networking sites. *The Educational Review, USA*. https://doi.org/10.26855/er.2019.10.004

Wang, J., Li, Y., & Rao, R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems, 17*(11), 759–783. https://doi.org/10.17705/1jais.00442

Winer, R. S. (2001). A Framework for Customer Relationship Management. *California Management Review, 43*(4), 89-105. https://doi.org/10.2307/41166102

Woetzel, L., Thomas, R., Barquin, S., & Devesa, T. (2021). *Future of Asia: The Future of Financial Services*. McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/future-of-asia-the-future-of-financial-services

Zacholska-Majer, N. (2025, October). *The Gmail Promotions Tab is evolving again! Google is rolling out "Deal Cards," a new feature designed to make your best offers stand out and be impossible to miss* [LinkedIn post]. LinkedIn. https://www.linkedin.com/posts/nataliazacholska_gmail-promotab-dealcards-activity-7384480089373241344-rVPs

Zenk-Möltgen, W., Akdeniz, E., Katsanidou, A., Naßhoven, V., & Balaban, E. (2018). Factors influencing the data sharing behavior of researchers in sociology and political science. *Journal of Documentation, 74*(5), 1053–1073. https://doi.org/10.1108/JD-09-2017-0126

Ziller, C., Loepp, B., Kindermann, B., Köchling, G., & Fadeeva, Y. (2025). Willingness to share personal data online: The role of social influence and sustainability. *Technology in Society, 83*, 102974. https://doi.org/10.1016/j.techsoc.2025.102974

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.