Separating privacy and security in online decision-making process: The case of Venmo

Gianluca Zanella
University of Texas at San Antonio
gianluca.zanella@utsa.edu

Mohsen Jozani
Augusta University
mjozani@augusta.edu

Morteza Safaei Pour
San Diego State University
msafaeipour@sdsu.edu

Abstract

The rise of peer-to-peer online financial services that attract users with social media features warrants a sharper distinction between security and privacy. While past research on online financial services focuses on the security of the transactions, the literature on online social media emphasizes the risks for the individual's privacy. Unfortunately, the two concepts are often considered as overlapping or, in some cases, as two dimensions of the same concept, thus making complex the study of the distinct roles of security and privacy in the decision-making process. We analyze the activity of $13,338$ *accounts on* `Venmo` *to explore the different roles of the two concepts in the decision to disclose financial transactions on online platforms. The results show that security concerns cause the users to opt-out of any public feeds, while users address their privacy concerns by limiting the amount of information disclosed. The findings and their impact are discussed.*

1. Introduction

Mobile money platforms that revolutionized the way we make payments have entered a new disruptive phase by adding a social aspect to the transactions. Besides being a "digital way of buying each other a drink at a bar" [1], the conjunction of online financial transaction and online social network is complex from a decision-making point of view because of its interdisciplinary nature. In particular, these platforms post each financial transaction into the user's activity stream, much like a `Twitter` feed. The dual nature, financial and social, of the user's decision to exchange money through these platforms warrants further study, for three main reasons.

First, security and privacy are often considered as overlapping concepts [2, 3] or as dimensions of the same concept [4]. The underlying assumption is that ordinary users fail to distinguish between security and privacy because they focus exclusively on practices regarding personal data protection carried out by the website. We contest this assumption by proposing that peculiar differences between security and privacy enable users to clearly distinguish between them. Specifically, privacy is linked to a set of legal requirements and best practices that enable individuals, groups, or institutions to claim full control on when, how, and to what extent information about them is communicated to others [5] . The growing body of literature reflects the increasing interest of both theory and practice on the disclosure of sensitive personal information that has been dramatically facilitated by the advent of online social media platforms [6]. This has increased the risks of personal information misuse, ranging from discrimination to identity theft, to stalking [7]. Conversely, security is referred as the technical guarantees that ensure that the personal information is transmitted and stored is such a way that third parties are not able to access or tamper with it [8]. Online users are increasingly aware of being exposed to security risks, such as fraud and misuse [9], during their online activities.

Second, past studies have not explored the interplay of security and privacy as distinct concepts in the online decision-making processes. Past research on online financial platforms focuses on user's perceived security of the new technologies, mainly perceptions regarding the reliability of the payment methods used and the mechanisms of data transmission and storage [10]. On the other hand, research on online social media platforms focuses on user's privacy concerns and how privacy affects aspects such as the obtainment, distribution, or the non-authorized use of personal information [11]. The Venmo platform provides a unique opportunity to explore the interplay of the two concepts.

Third, the study of `Venmo` transactions provides the opportunity to study the effect of user's perceptions and attitudes on their online behavior. Often, past studies measure user's intent or laboratory-measured behavior through surveys or controlled experiments, that

URI: https://hdl.handle.net/10125/79707
978-0-9981331-5-7
(CC BY-NC-ND 4.0)

can introduce hypothetical bias [12]. In our study, we analyze real-life user's decision-making process to improve validity and generalizability of our results.

The rise of mobile payment apps, such as Venmo, PayPal, Zelle, ApplePay, Google Wallet, Visa Checkout, and Stripe, reflects the users growing interest in peer-to-peer financial services. The ability to directly transact with little or no intermediation by third parties appeals to individuals and small businesses, given its intrinsic efficiency, reduced overhead costs, and lack of regulation. With nearly 70 million active users, Venmo is one of the largest and most successful players in this market [13]. Venmo's popularity is largely due to its unique combination of financial transaction and social media capabilities. Despite serious privacy issues regarding public engagement on the app, about 90% of all the transactions on Venmo are public and users open the app more for social interactions rather than to make actual payments [14]. These unique characteristics provide a great context for simultaneously examining user's privacy and security concerns. Because of its dual nature, Venmo affect both individual privacy and security which, in turn, makes it an ideal case to answer our main research question: RQ: Are the roles of privacy and security different in the user's decision-making process? The rise of popularity of these hybrid platforms, such as Ali Pay and WeChat Pay, in conjunction with their dual nature make more relevant the research question.

In this study, we collect data from 13,338 profiles on Venmo and their respective reviews of the Venmo app on Google Play. Using a supervised natural language processing-based classifier, we identify each user's attitude toward utility benefits along with their security and privacy concerns. Finally, we apply a regression model with selection estimator to analyze the effect of privacy and security concerns on the user's decisions. The results support the proposed hypotheses regarding the differential roles of privacy and security on the decision-making process. The findings of this research benefits both theory and practice, enabling further studies on how security and privacy play different roles in shaping the perspective of online platform users. The rest of the paper will present a brief theoretical introduction, the design of this study, the results, and a brief discussion and conclusion section.

2. Theoretical Background

We review the theoretical background regarding privacy, security, and interplay of privacy and security.

2.1. Privacy

The concept of privacy at individual and social level has long been studied by scholars, and the arrival of online social networks has increased the concerns and posed new threats to individuals' privacy, ranging from identity theft to stalking and discrimination [7]. Westin [5] has defined privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others", thus highlighting the double nature of privacy as information and control of it. The technological innovations of the past few years have changed the breadth and depth of potential exposure of private information, mainly because of the increased number of third parties involved in the provision of mobile-enabled services [15]. The growing perception of these risks is reflected in people's increasing concerns about their privacy and the collection and use of their personal information [16]. However, despite of the great concerns about the risks related to self-disclosure and little confidence in the possibility to control who will access their online personal information, users are willing to share information online [17].

A growing body of literature proposes explanations of the roles of privacy and privacy concerns on user's online behavior. There is general agreement on the fact that active participation in online social networks or communities satisfies individual's fundamental needs, such as the need for diversion and entertainment [18], social relationships [19], identity construction [20], social support, social validation, self-presentation [21], and social capital [22, 23]. The perceived benefits of belonging to a social collective often outweighs the perceived hazards of data misuses [17], namely the user's privacy concerns. The decision-making process follows an exchange paradigm in which the perceived benefits are evaluated against the potential risks for the individual's privacy [24]. The result of the (privacy) calculus is surprisingly in favor of the online disclosure of private information that rewards with social benefits, even in presence of serious risks to the individual privacy [25]. Perhaps, past studies find that privacy concerns negatively affect, but do not prevent, online self-disclosure [26]. Therefore, to protect their privacy, users decide to publicly disclose less information (or less often) or to restrict access to the information.

2.2. Security

In the past two decades, the financial sector has adopted cloud-based technological innovations that have reshaped the ways financial institutions interact and

engage customers. One of the most recent innovations is the mobile (digital) wallets. There is a broad agreement that convenience is the most critical factor in the adoption of new online payment technologies [27]. Indeed, users perceive greater benefits from the adoption of mobile wallets compared to alternative payment methods, for many reasons. First, users do not need to memorize or input PINs or other pieces of information, thus saving time and effort. Second, they do not need to carry cash or credit cards, thus saving the need for a physical wallet. Furthermore, the transaction is contactless and there is no need to show or hand the credit card, thus contributing to the perception of a secure transaction.

As in the case of privacy in social media, these perceived benefits are also countered by related risks. Indeed, the rise of online payment platforms as payment methods more convenient than the classic credit/debit cards is paralleled by the rising concerns about the security of these interactions [28]. Perhaps, the perception of insecurity connected to housing financial data within the cloud dominates the existing financial cloud literature [29] and creates concerns among users that prevent a wider usage of these services [30]. User's concerns focus on the possibility that financial data might be exploited for fraudulent use [10]. Information security can be defined as the task of protecting the confidentiality, integrity, and availability [8] of information. Perceived security emerges as a critical factor to build consumer's trust in online financial services. Trust, in turn, contributes to customer loyalty to a financial service, which affects their use intention and behavior [4]. To build trust, customers require the online platforms to show technical competence in managing transactions and storing data. For example, user's concerns focus on safely transmitting and storing their information [31]. Higher concerns regarding the security of a platform correspond to a lower trust. That in turn, corresponds to lower rate of adoption of such service.

2.3. Venmo: Interplay of Privacy and Security

The global market for mobile payment applications is growing at a fast pace, with Ali Pay counting more than 1.2 billion users and WeChat Pay with more than 1.151 billion users. Apple Pay, PayPal, Samsung Pay, Amazon Pay, and Google Pay follow behind [32]. Although, the Department of Homeland Security classifies financial services as critical sectors [33] and the market for digital wallets becomes increasingly populated, some platforms, such as Ali Pay and WeChat Pay, are exploring the opportunity to merge the financial services with online social media features. Users can publicly post their financial transactions just like they publicly share or get the bill at the restaurant.

The most prominent example of such hybrid nature is Venmo, a virtual fiscal intermediary between users that exchange funds among one another, with the addition that the users can add emojis to describe the transaction, which is posted on the user's public feed. Depending on the level (public, friends, private), the transaction's metadata may indicate the requester and the payer, the date, and the description of the transaction. Users can invite friends, allow the app to access their contacts stored on their phones, or connect the app to their Facebook account, which imports a complete friend list that are added as payment contacts. Other users can comment or "like" the transactions.

Like almost all internet-connected applications, Venmo has been vulnerable to security breaches. Reportedly, cybercriminals use a variety of techniques such as voice and in-person phishing scams, fake sale, or reverse transaction scams, or exploit Bluetooth vulnerabilities to steal funds from users' Venmo accounts [34]. To address their security concerns, users may enable biometric and two factor authentication, use stronger passwords and limit the audience of their profile feeds.

From a privacy perspective, the user's feed can reveal information such as parties involved, date, and the reason for transaction. The publicly available information represents a significant risk for the individual's privacy. Monitoring Venmo's feed, media reporters have revealed political scandals [35], and managed to discover the account information of the US president in less than 10 minutes [36]. The only way to minimize the risk is to limit the number of transactions, exchange money only with familiar people, and avoid posting sensitive details in transaction descriptions, thus minimizing the information exposed to the public. Despite such privacy issues, about 90% of all Venmo transactions are public and users open the app more for social interactions rather than to make actual payments [37].

From examining the features of Venmo it becomes clear that the decision of using the platform raises concerns about both security and privacy. Security concerns involve the financial aspect of the usage, while privacy concerns relate to its social aspect. Perhaps, the underlying decision-making process is complex because merges different types of behavior, which requires to account for different types of perceptions and attitudes.

As discussed earlier, both social rewards and privacy concerns derive from online social activity. Past research found that the user's strategy to mitigate

Table 1. Key points about security vs. privacy

Security	Privacy
Data Confidentiality (Secure Transmission)	Audience Control (who has access to Private Data)
Data Integrity (Secure Storage)	Extent Control (to what extent third parties access data)
Data Availability (Secure Access)	Timing Control (when third parties can access data)

the privacy concerns is to decrease the amount of information released or to restrict the access to it [26, 25]. Therefore, we propose:

- H1.1: Privacy concerns is negatively related to online self-disclosure of private information.
- H1.2: Privacy concerns is positively related to the decision to change the account setting to "private".

Security concerns, on the other hand, relate to the technical and procedural ability of the platform to safely transmit and store their information. User's strategy to cope with security concerns is to opt-out from the platform or from the specific functionality [30]. In Venmo case, we have discussed that the flag "private" opts-out the user from posting on the feed. Thus, we propose:

- H2: Security concerns is positively related to the decision to change the account setting to "private".

We expect that security concerns do not affect the number of transactions posted on the user's feed because security concerns the safety of transmission and storage of information, not the content of the information (see Table 1).

Finally, users are increasingly forced to accept the loss of their privacy and security in return for the benefits they obtain from their online presence [38]. The privacy literature recognizes utility benefits as one of the major drivers of users' information disclosure, especially in the context of social media enabled apps [15]. Utility benefits refer to the usefulness and convenience users may perceive as a result of engaging with a certain technology [39]. Venmo enables users to complete transactions quickly and free of charge. It makes it easy for individuals to split bills, request money, or pay one another without needing to carry cash. Therefore, we propose:

- H3.1: Perceived utility is positively related to online self-disclosure of private information.

Both security and privacy literature identify perceived utility as a major driver of users' information disclosure behavior on online platforms. Users would be more active on a given platform when engagement is effortless. Besides, the convenience and functionality that the technology delivers will increase user satisfaction and higher degree of satisfaction is associated with increased user activity and continued use [40]. Therefore, we propose:

- H3.2: Perceived utility is negatively related to the decision to change the account setting to "private".

3. Methodology

This study combines deep learning-based NLP with econometric models to investigate the differential roles of privacy and security concerns in decision-making process of individuals. First, we describe the dataset and our data matching approach. Next, we discuss our data processing method and introduce the study measures. Finally, we present the analysis results.

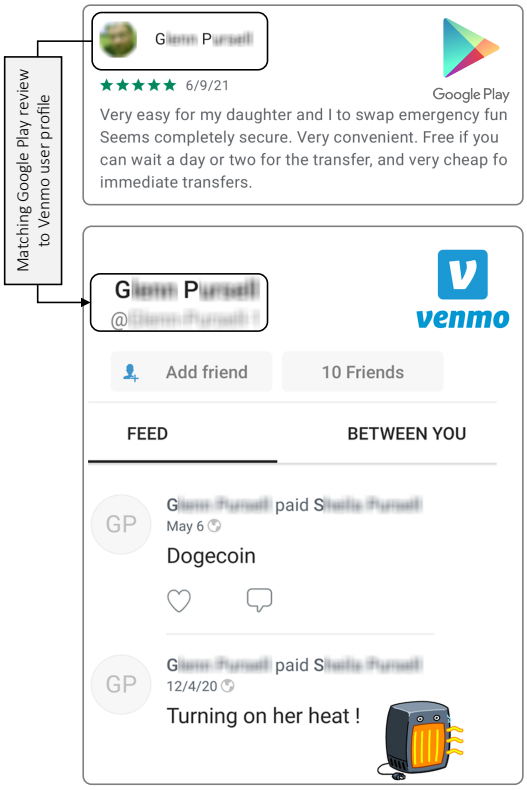
3.1. Data

To build the dataset for this study, we matched user reviews on *Google Play* with Venmo user profiles. The data were collected between Jan 09 and Jan 21, 2019. First, using a web scraper we collected all the reviews for the Venmo app posted on *Google Play* (34,272 reviews posted between August 21, 2010, and April 21, 2018). Then, based on usernames, we tracked users who posted reviews on *Google Play* to find their Venmo profiles [1] (Figure 3.1).

Google provides users with the option to post reviews anonymously, these reviews appear with the username *"A Google User"*. After removing the anonymous reviews, we searched for 45,438 *Google Play* usernames on Venmo's website to obtain the profile data of users who had posted the reviews. To make sure we would collect the data for the right user, we only included users for whom there was only one match on Venmo's search results page. We were able to match 13,338 users from *Google Play* with Venmo profiles. 77 percent of the user profiles were public, and 23 percent were set to private.

[1] This study does not meet the definition of human subject research per federal regulations and is exempt from IRB review since (a) data is publicly available, and (b) unit of analysis is each review text rather than the individual (National Institutes of Health, 2016; Office for Human Research Protections, 2016).

Figure 1. Matching Google Play usernames to Venmo profiles



3.2. Data Processing

We leveraged semantic indexing (text classification) to understand what people are seeking from their reviews. Using manual labeling, we labeled $3,612$ reviews with labels consisting of "privacy concern" (372), "security concern" (364) and "utility" (549) labels. We divide the resulted labeled data set to 60%, 20% and 20% portions respectively for training $(2,889)$, validation (723) and testing (723).

Subsequently, we leveraged Google BERT (Bidirectional Encoder Representations from Transformers) [41], a pre-training transformer-based method for Natural Language Processing (NLP) that shows outstanding performance in various NLP tasks. BERT operates in two stages. First, it pre-trains a language representation using a vast quantity of unlabeled data. The pre-trained model will then be fine-tuned in a supervised manner to accomplish various supervised tasks using a limited quantity of labeled training data.

For our text classification task we used `bert-base-uncased` consisting of 12-layer, 768-hidden, 12-heads, 110M parameters that pre-trained on unlabeled data extracted from English Wikipedia with 2,500M words. Subsequently, we trained three distinct models by fine tuning it on our manually labeled training dataset to achieve three binary classification tasks (to identify privacy concern, security concern and convenience aspects in each review texts). The pre-trained models comes with their own text cleaning and tokenizer. The performance metrics for BERT present significant improvement over three other based lines (TD-IDF + {SVM, Logistic regression, Naïve Bayes}) [42] that are reported in Table 2. Due to the class imbalance, F1-micro and F1-Macro are better metrics to compare the models [43]. BERT model achieved F1-micro and F1-Macro of $(0.9599, 0.9889)$, $(0.9830, 0.9930)$ and $(0.9433, 0.9723)$ respectively for privacy, security and convenience classes.

3.3. Measures

To make sure we would collect the data for the right user, we only included users for whom there was only one match on `Venmo`'s search results page. We were able to match 13,338 users from Google Play with `Venmo` profiles. For each review, we operationalize the study variables as follows: *public* is a dummy variable that shows whether a user has set their profile to private. 77 percent of the profiles were public, and 23 percent were set to private.

public_transact is only available for public profiles and shows the number of transactions (feeds) for each profile. Taking a calculus perspective, we consider *privacy* and *security* as costs, and *utility* as the benefit of disclosure behavior. For each review, the value for these aspects can be recorded as either zero or one. If a review has a negative sentiment towards *privacy* or *security*, those aspects are coded as one. And every time there is a positive mention of the utility, convenience, or functionality of the app, the *utility* aspect is coded as one. Consistent with the calculus perspective, we are comparing the costs (i.e., negative *privacy* and *security*) to the benefits (i.e., positive *utility*) of self-disclosure. We also control for the effect of variables that can influence the number of transactions. *Friends* indicates the number of friends each user has on `Venmo`. *Memdays* is the number of days since a user has joined the platform and we consider this variable as a measure of app experience. Finally, we chose not to include app review rating as a control variable since past research suggests that review rating which is a post adoption metric that signifies user satisfaction, can highly correlate with their perception of utility of a mobile app [44]. Indeed, Figure 2 shows an almost perfect linear relationship between star rating and perceived utility. Table 3 shows our study variables.

Table 2. Performance metrics of text classification trained models for privacy concern, security concern and convenience seeking classes.

	Privacy					Security					Convenience				
Model	Accuracy	Precision	Recall	F1-Macro	F1-Micro	Accuracy	Precision	Recall	F1-Macro	F1-Micro	Accuracy	Precision	Recall	F1-Macro	F1-Micro
BERT	0.9889	1.00	0.86	0.9599	0.9889	0.9930	0.99	0.95	0.9830	0.9930	0.9723	0.94	0.87	0.9433	0.9723
TD-IDF+SVM	0.9409	0.97	0.52	0.8205	0.9409	0.9704	0.92	0.73	0.8978	50.9704	0.9391	0.97	0.65	0.8708	0.9391
TD-IDF+LR	0.9695	0.96	0.77	0.9200	0.9695	0.16	140	3	4	5	0.9584	0.96	0.96	0.9220	0.9584
TD-IDF+NB	0.9095	1.00	0.23	0.6654	0.9095	0.9557	1.00	0.49	0.8191	0.9557	0.8976	0.96	0.39	0.7499	0.8976

Table 3. Study Variables

Variable	Definition
public	The Venmo profile is public.
public_transact	Number of transaction feeds on Venmo profile (none for private profiles).
privacy	Perceived App's privacy ($n = 319$).
security	Perceived App's security ($n = 157$).
utility	Perceived App's utility ($n = 6870$).
friends	Number of friends on Venmo.
memdays	Days of Venmo membership until the day of data collection.

3.4. Analysis

To test our hypotheses and jointly estimate (a) the likelihood of having a public profile; and (b) the degree of public transactions, we use Heckman's two-stage estimation model [45]. Our dataset contains the number of transactions only for users who have public profiles. Privacy conscious users are more likely to set their profiles to private, causing concerns for selection bias in the sample. Heckman's two-stage model was chosen to address this issue. In this approach, we first use a Probit model to estimate the selection (i.e., the likelihood of having a public Venmo profile). This Probit model also calculates a correction factor (the inverse Mills ratio) that is included to correct for the sample selection issue in the final OLS model where we estimate the number of transaction feeds for each user.

Both equations are estimated using the number of public transactions as the dependent variable.

We define the number of public transactions as a function of user's attitude regarding the privacy and security risks, as well as utility benefits of `Venmo` along with the star rating they post on `Google Play`. Besides, we control for uses' duration of membership and their number of friends. Whereas the likelihood of public transactions (the likelihood of setting one's profile to public) is a function of privacy and security risks and utility benefits. Thus, we formally define our econometric model as:

$$public\_transact = \beta_0 + \beta_1 privacy + \beta_2 security + \beta_3 utility + \beta_4 star\_rating + \beta_5 friends + \beta_6 memdays + u_1$$

And we assume the public_transact is observed if:

$$\gamma_0 + \gamma_1 privacy + \gamma_2 security + \gamma_3 utility > 0$$

Table 4. Results of the Heckman Model

Variable	Selection Model DV: *public*	Regression Model DV: *public_transact*
privacy	-0.697^{***} (0.07)	-17.246^{***} (4.88)
security	-0.392^{***} (0.10)	-3.190 (5.18)
utility	0.049^{*} (0.02)	0.591 (0.97)
friends	—	0.134^{***} (0.00)
memdays	—	0.013^{***} (0.00)
constant	0.729^{***} (0.02)	20.899^{***} (3.37)
Obs.	3,111 (Private Accounts)	10,227 (Public Accounts)
Total Obs.	13,888	
log likelihood	-61377.61	

Notes: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$
Standard errors in parentheses.

Table 5. VIF Test Results

Variable	VIF	1/VIF
privacy	1.00	1.00
security	1.00	1.00
utility	1.00	1.00
friends	1.09	0.92
memdays	1.09	0.92
Mean VIF	1.04	

Table 4 shows the result of the two stages of the Heckman selection model.

To ensure the validity of our results, we performed variance inflation factor (VIF) test and as shown in Table 5, the VIF values are well below the acceptable threshold of 10. Therefore, we can conclude that our model does not suffer from the problem of multicollinearity.

4. Findings

The two-stage Heckman's selection model provides two different sets of results. First, it identifies the variables that significantly affect the choice to identify the account as "private" (see columns "Selection Model" in Table 4). Because of our variable's choice (0 corresponds to private and 1 to public), the selection model focuses on the choice to declare "public" the account and its transactions. The results confirm our proposed hypotheses. Users concerned about their privacy are more likely to decide to hide their transactions by declaring "private" the account, thus supporting H1.2. Moreover, users concerned about their security are more likely to decide to hide all their transactions by declaring "private" the account, thus supporting H2. Finally, users with higher perceived utility are more likely to keep their accounts public, thus confirming H3.2.

Second, the Heckman's regression model identifies the variables that significantly affect the number of financials transactions made through the Venmo platform. The results show that users concerned about their privacy are less likely to disclose information about their financial transactions, thus supporting H1.1. Finally, the perception of utility is not significantly related to the number of public transactions, thus failing to support H3.1. To provide an overview of the results of our analysis, we summarized the outcome of the hypotheses testing in Table 6. The next section discusses the results and the implications of our study.

Table 6. Hypothesis Testing Results

	Hypothesized relationship	Result
H1.1	Privacy concerns is negatively related to online self-disclosure of private information.	Supported
H1.2	Privacy concerns is positively related to the decision to keep private the information.	Supported
H2	Security concerns is positively related to the decision to change the account setting to "private".	Supported
H3.1	Perceived utility is positively related to online self-disclosure of private information.	Not supported
H3.2	Perceived utility is negatively related to the decision to keep private the information.	Supported

5. Discussion and Conclusions

This paper focuses on the differences between the role of perceived online privacy and perceived online security in the decision-making process. By merging data from Google Play and Venmo user's feeds, we were able to apply the Heckman selection model for analyzing the role of privacy and security on the user's decisions of making public financial transactions. Venmo is one of the increasingly popular online financial services that allow users to publicly exchange money in a social context. The results of our analysis confirm that privacy and security play a different role in shaping user's strategy to address the concerns regarding the misuse of their personal information. Users concerned about the security of their data use the security features available on the platform that can prevent the exploitation of their data. In the case of Venmo, security concerns drive the decision to change the account settings to "private", thus completely hiding the activity from the public eyes. A possible takeaway from our analysis is that the decision to "opt-out" is the only strategy enacted by people with high security concerns. Indeed, the security concerns do not affect the number of transactions that users post on their feeds. Conversely, users concerned about their privacy focus to decreasing the amount of information publicly available. In fact, our findings show that privacy concerns drive both the decision to change to "private" settings and the decision to limit the use of the platform. Perhaps, this finding aligns with literature that generally agrees on the fact that reduced exposure of information is one of the user's strategies to address privacy concerns. More interestingly, our results shows that security concerns do not affect the amount of information disclosed on Venmo, thus supporting the different role of perceived security and privacy in the decision-making process. The users more concerned about their security are more likely to decide to opt-out from public disclosure on Venmo. Finally, while we found that the perception of utility increases the likelihood of having a public Venmo account. However, the perceived utility does not relate with the number of transactions disclosed. A potential explanation can be that the perceived utility focus on the benefits coming from the combination of social media and financial services. This triggers the decision to keep public the account but does not affect the amount of information disclosed. Indeed, our post hoc analysis reveals that many individuals who enjoy the convenience and utility of the app are also concerned about its privacy risks, as shown in the example reviews below.

"An easy and quick way to pay. The dark side is every transaction is broadcast to friends and family - no privacy."

"It's convenient but I find it disturbing that it tries to

Table 7. Co-occurrence Matrix

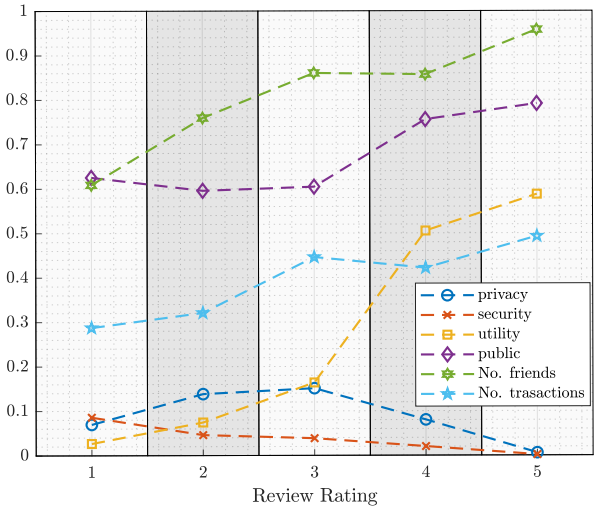
	Utility	Privacy	Security	Public
Utility	6870 (100%)	–	–	–
Privacy	101 (32%)	319 (100%)	–	–
Security	28 (18%)	9 (6%)	157 (100%)	–
Public	5350 (52%)	166 (2%)	98 (1%)	10226 (100%)

be a social app. I just want to send money. I don't need to see who else sent money to each other. It's stupid."

The co-occurrence matrix (Table 7) shows that almost 32 percent of users who complain about privacy are in fact content with the utility and convenience that `Venmo` delivers. Perhaps, the perceived utility of the app contributes to the decision to keep public the activity on the platform. Indeed, both the financial service and the social aspect of it can be interpreted as utilitarian functionalities that combined contribute to the user's social life. After this decision is done, users with higher privacy concerns can limit their public exposure by decreasing the number of transactions publicly posted on the platform. This may also contribute to explain why past literature found that integrating hedonic features into utilitarian apps results in lower app usage [46]. In fact, hedonic features on utilitarian apps can raise user's perceived security concerns that, in turn, negatively affect app's usage.

Moreover, 78 percent of users who express positive utility in their reviews have public accounts, while the percentage of public accounts for those with security and privacy risks are 62 percent and 52 percent, respectively. Figure 5 shows the breakdown of aspects and the number of transactions based on the star rating of the reviews.

Figure 2. The relationship between user's average discussion of aspects and their ratings of the app.[2]



5.1. Implications for research

We proposed a new empirical study that contributes to the growing body of literature on privacy and security in online decision-making processes. Although past literature often mixes the concepts of privacy and security, we found that the users perceive the two concepts as different, and act accordingly. This affects future research in different ways. First, our findings should trigger a revision of privacy scales, that should account only for perceived threats to the user's privacy. Often, the two concepts are overlapped [47] or merged into a common construct [4]. The findings of this study show that the two concepts should be assumed as different and used accordingly to their theoretical nature to increase the validity of the results. Second, our findings that users concerned about security tend to use the control features of the platform may explain why past research found that, paradoxically, user's perceived control ends up increasing their willingness to disclose sensitive information [48]. Perhaps, users' perceived control addresses security concerns, leaving perceived privacy concerns dealing with self-disclosure.

5.2. Implications for practice

The findings of our study contribute to a better understanding of the user's decision-making processes. This informs practitioners in many ways. First, the concepts of security and practice are perceived in different ways from a user's perspective. Users address security concerns through asserting control on the access, while users concerned about privacy tend to use mitigating strategy, such as restraining to use the services. Online platforms should embed such differences into the design of their interfaces. For example, they can provide the users with different tools for security and privacy, designed to match user's strategies to address each concern. Also, managers looking for improving user's engagement should understand the different effect of privacy and security on user's behavior. Our findings show that security concerns are addressed by "opting-out" of the public feeds, but this may not affect their use of the services. Conversely, users concerned about privacy tend to limit the use of the services. Therefore, offering a "private" choice would be advisable for security-concerned users, while tools to limit the amount of information posted on public feeds may be a better strategy for privacy-concerned users.

[2] all the variables have been re-scaled to fit in the figure (e.g., No. friends and No. transactions are divided by 100.)

5.3. Limitations and Future Research

Although the design of our research based on actual behavior increases the validity of our finding, we are aware of some limitations that should be addressed in future research. First, we recognize that our sample represents only actual users of this platform and does not consider users that decided to close their accounts. Indeed, we plan to collect information on the accounts that have been closed since we collected the data, thus providing a more general approach to the study of the decision-making processes. Second, the sample has been collected from one specific platform, and future studies should include more platforms to verify our findings. Finally, our results show that users adopt different strategies to address privacy and security concerns, thus suggesting that user's perceptions in matter of security and privacy differ. However, it does not provide an explanation on why. Future research should explore the differences between user's attitudes toward security and toward privacy to explain why the adopted strategies are different.

In conclusion, our study shows that users perceive and address concerns about privacy and security in different ways. These results inform scholars and practitioners on the opportunity to improve their respective approaches by assuming that the two concepts are different and therefore, they must be conceptualized separately.

References

[1] S. Goldmacher, "Cash condolences, and beer emojis, via venmo when campaigns fizzle," *The New York Times*, pp. 17–17, 2020.

[2] E. D. Matemba and G. Li, "Consumers' willingness to adopt and use wechat wallet: An empirical study in south africa," *Technology in Society*, vol. 53, pp. 55–68, 2018.

[3] P. McCole, E. Ramsey, and J. Williams, "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns," *Journal of Business Research*, vol. 63, no. 9-10, pp. 1018–1024, 2010.

[4] C. Flavián and M. Guinalíu, "Consumer trust, perceived security and privacy policy," *Industrial management & data Systems*, 2006.

[5] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, p. 166, 1968.

[6] H. R. Rao, N. Vemprala, P. Akello, and R. Valecha, "Retweets of officials' alarming vs reassuring messages during the covid-19 pandemic: Implications for crisis management," *International Journal of Information Management*, vol. 55, p. 102187, 2020.

[7] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71–80, 2005.

[8] R. Mekovec and Ž. Hutinski, "The role of perceived privacy and perceived security in online market," in *2012 Proceedings of the 35th International Convention MIPRO*, pp. 1549–1554, IEEE, 2012.

[9] A. D. Miyazaki and A. Fernandez, "Internet privacy and security: An examination of online retailer disclosures," *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 54–61, 2000.

[10] S. Jones, M. Wilikens, P. Morris, and M. Masera, "Trust requirements in e-business," *Communications of the ACM*, vol. 43, no. 12, pp. 81–87, 2000.

[11] H. Wang, M. K. Lee, and C. Wang, "Consumer privacy concerns about internet marketing," *Communications of the ACM*, vol. 41, no. 3, pp. 63–70, 1998.

[12] I. Ajzen, T. C. Brown, and F. Carvajal, "Explaining the discrepancy between intentions and actions: The case of hypothetical bias in contingent valuation," *Personality and social psychology bulletin*, vol. 30, no. 9, pp. 1108–1121, 2004.

[13] C. Scott, "Venmo to Charge Users for Selling Goods and Services," 2021. [Online; accessed 3-September-2021].

[14] M. Lev-Ram, "PayPal's CEO on Venmo: Don't Mess Up the 'Special Magic'," 2017. [Online; accessed 3-September-2021].

[15] M. Jozani, E. Ayaburi, M. Ko, and K.-K. R. Choo, "Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective," *Computers in Human Behavior*, vol. 107, p. 106260, 2020.

[16] M. Madden, "Public perceptions of privacy and security in the post-snowden era," *Pew Research Center*, 2014.

[17] G. Blank, G. Bolsover, and E. Dubois, "A new privacy paradox," in *Proceedings of the Annual Meeting of the American Sociological Association 2014*, pp. 1–34, Citeseer, 2014.

[18] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes, "Facebook and online privacy: Attitudes, behaviors, and unintended consequences," *Journal of computer-mediated communication*, vol. 15, no. 1, pp. 83–108, 2009.

[19] C. Lutz and P. Strathoff, "Privacy concerns and online behavior–not so paradoxical after all? viewing the privacy paradox through different theoretical lenses," *Viewing the Privacy Paradox Through Different Theoretical Lenses (April 15, 2014)*, 2014.

[20] C. R. Berger and R. J. Calabrese, "Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication," *Human communication research*, vol. 1, no. 2, pp. 99–112, 1974.

[21] H. Lee, H. Park, and J. Kim, "Why do people share their context information on social network services? a qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk," *International Journal of Human-Computer Studies*, vol. 71, no. 9, pp. 862–877, 2013.

[22] N. B. Ellison, C. Steinfield, and C. Lampe, "The benefits of facebook "friends:" social capital and college students' use of online social network sites," *Journal of computer-mediated communication*, vol. 12, no. 4, pp. 1143–1168, 2007.

[23] N. B. Ellison, C. Steinfield, and C. Lampe, "Connection strategies: Social capital implications of facebook-enabled communication practices," *New media & society*, vol. 13, no. 6, pp. 873–892, 2011.

[24] F. S. Houston and J. B. Gassenheimer, "Marketing and exchange," *Journal of marketing*, vol. 51, no. 4, pp. 3–18, 1987.

[25] C. Hallam and G. Zanella, "Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards," *Computers in Human Behavior*, vol. 68, pp. 217–227, 2017.

[26] A. Acquisti and J. Grossklags, "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior," in *2nd Annual Workshop on Economics and Information Security-WEIS*, vol. 3, pp. 1–27, Citeseer, 2003.

[27] G. Aydin and S. Burnaz, "Adoption of mobile payment systems: A study on mobile wallets," *Journal of Business Economics and Finance*, vol. 5, no. 1, pp. 73–92, 2016.

[28] W. Venters and E. A. Whitley, "A critical review of cloud computing: researching desires and realities," *Journal of Information Technology*, vol. 27, no. 3, pp. 179–197, 2012.

[29] A. Benlian and T. Hess, "Opportunities and risks of software-as-a-service: Findings from a survey of it executives," *Decision support systems*, vol. 52, no. 1, pp. 232–246, 2011.

[30] S. M. Furnell and T. Karweni, "Security implications of electronic commerce: a survey of consumers and businesses," *Internet research*, 1999.

[31] L. V. Casaló, C. Flavián, and M. Guinalíu, "The role of security, privacy, usability and reputation in the development of online banking," *Online Information Review*, 2007.

[32] C. Mombeuil and H. Uhde, "Relative convenience, relative advantage, perceived security, perceived privacy, and continuous use intention of china's wechat pay: A mixed-method two-phase design study," *Journal of Retailing and Consumer Services*, vol. 59, p. 102384, 2021.

[33] M. Husák, N. Neshenko, M. S. Pour, E. Bou-Harb, and P. Čeleda, "Assessing internet-wide cyber situational awareness of critical sectors," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1–6, 2018.

[34] A. Weaver, "Yes, your venmo account can be hacked – here's how to protect yourself," *hacked.com*, 2021.

[35] J. Pagliery and R. Sollenberger, "Gaetz paid accused sex trafficker, who then venmo'd teen," *www.thedailybeast.com*, 2021.

[36] M. Pengelly, "Joe biden's venmo account discovered in 'less than 10 minutes' – report," *theguardian.com*, 2021.

[37] M. Lev-Ram, "Paypal's ceo on venmo: Don't mess up the 'special magic'," *fortune.com*, 2017.

[38] A. L. Young and A. Quan-Haase, "Privacy protection strategies on facebook: The internet privacy paradox revisited," *Information, Communication & Society*, vol. 16, no. 4, pp. 479–500, 2013.

[39] V. Venkatesh and S. A. Brown, "A longitudinal investigation of personal computers in homes: Adoption determinants and emerging challenges," *MIS quarterly*, pp. 71–102, 2001.

[40] Y. H. Kim, D. J. Kim, and K. Wachter, "A study of mobile user engagement (moen): Engagement motivations, perceived value, satisfaction, and continued engagement intention," *Decision support systems*, vol. 56, pp. 361–370, 2013.

[41] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," *arXiv preprint arXiv:1810.04805*, 2018.

[42] H. Moradi, W. Wang, and D. Zhu, "Online performance modeling and prediction for single-vm applications in multi-tenant clouds," *IEEE Transactions on Cloud Computing*, 2021.

[43] N. Bendre, N. Ebadi, J. J. Prevost, and P. Najafirad, "Human action performance using deep neuro-fuzzy recurrent attention model," *IEEE Access*, vol. 8, pp. 57749–57761, 2020.

[44] W. Tafesse, "The effect of app store strategy on app rating: The moderating role of hedonic and utilitarian mobile apps," *International Journal of Information Management*, vol. 57, p. 102299, 2021.

[45] J. J. Heckman, "Sample selection bias as a specification error," *Econometrica: Journal of the econometric society*, pp. 153–161, 1979.

[46] T. Mettler, F. Wortmann, and K. Flüchter, "How do hedonic design features influence an application's usage," 2014.

[47] I. Arpaci, K. Kilicer, and S. Bardakci, "Effects of security and privacy concerns on educational use of cloud services," *Computers in Human Behavior*, vol. 45, pp. 93–98, 2015.

[48] L. Brandimarte, A. Acquisti, and G. Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social psychological and personality science*, vol. 4, no. 3, pp. 340–347, 2013.