International Journal of Human–Computer Interaction

ISSN: 1044-7318 (Print) 1532-7590 (Online) Journal homepage: www.tandfonline.com/journals/hihc20

To Bid or Not to Bid: Using Auctions to Understand User Valuation of Digital Accounts

Shubham Singh, Jackie Hu , Cormac Herley , Elissa M. Redmiles , Siddharth Suri & Oshrat Ayalon

To cite this article: Shubham Singh, Jackie Hu , Cormac Herley , Elissa M. Redmiles , Siddharth Suri & Oshrat Ayalon (11 Mar 2026): To Bid or Not to Bid: Using Auctions to Understand User Valuation of Digital Accounts, International Journal of Human–Computer Interaction, DOI: 10.1080/10447318.2026.2634976

To link to this article: https://doi.org/10.1080/10447318.2026.2634976

INTERNATIONAL JOURNAL OF HUMAN–COMPUTER INTERACTION
https://doi.org/10.1080/10447318.2026.2634976

To Bid or Not to Bid: Using Auctions to Understand User Valuation of Digital Accounts

Shubham Singh[a], Jackie Hu[b], Cormac Herley[c], Elissa M. Redmiles[d], Siddharth Suri[c] and Oshrat Ayalon[e]

[a]The Data Science Institute, University of Chicago, Chicago, USA; [b]School of Information, University of Michigan, Ann Arbor, USA; [c]Microsoft Research, Microsoft, Redmond, USA; [d]Department of Computer Science, Georgetown University, Washington, USA; [e]Information Systems Department, Faculty of Computer and Information Science, University of Haifa, Haifa, Israel

ABSTRACT

Most digital service providers offer free accounts to users and then generate revenue by monetizing the data provided by them. However, the way users derive value from their accounts and what factors affect their valuation needs further scrutiny. In this study, we used a novel auction-based methodology to understand users' valuation of their digital accounts and how this relates to their security decision-making. We conducted a behavioral economics study with $n = 66$ participants at two university campuses to assess their reasons for being willing to provide researchers with their digital accounts' credentials in exchange for money – hence, compromising security and privacy protection – and what contextual factors governed their decision-making. We found that the main factors influencing participants' valuation of their accounts were their beliefs about data and privacy, envisioned threats, and the account properties and utility. Finally, we discuss the context-dependent nature of these factors and their implication on future research.

KEYWORDS

Security; privacy; decision-making; auctions

1. Introduction

As more aspects of our lives now take place in an increasingly digital environment, we use many digital services for everyday tasks, such as communication, food delivery, and transportation. While such services ease up our lives in one way, the increasing use of digital services also means more personal data are stored and processed digitally, and need to be protected from known and mainly unknown entities. Security researchers have devised many tools and mechanisms to help users prevent their accounts from being compromised, such as 2-factor authentication and password managers. However, efforts to persuade users to utilize these tools or follow security best practices have had limited impact. Although some of the tools (e.g., password managers) are adopted now by more users than before (McClain et al., 2023), other practices that are considered insecure, like password reuse, still remain commonly used (Google, 2023).

Prior work has explored influences on users' security behavior, identifying various factors. Often, security is not users' main concern and imposes costs users are not always willing to bear (Acquisti et al., 2018; Duggan et al., 2012). While costs like choosing strong passwords are concrete, the benefits of secure behavior are less clear. Awareness of security risks also shapes behavior; for instance, examining users' security behavior in the context of COVID − 19 scams, it was found that general security awareness was one of the strongest determinants of protective security behavior (Al-Balushi et al.,

CONTACT Oshrat Ayalon oayalon@is.haifa.ac.il Information Systems Department, Faculty of Computer and Information Science, University of Haifa, 199 Aba Khoushy Ave., Mount Carmel, Haifa, 3498838, Israel

Supplemental data for this article can be accessed online at https://doi.org/10.1080/10447318.2026.2634976.

2024). Other factors include the usability of security mechanisms (Ibrahim et al., 2010) and the context, such as using public devices (Munyendo et al., 2023).

One motivation for understanding users' security perceptions and behavior is to discover a way to encourage them to adopt security mechanisms. However, security researchers face challenges measuring security decisions in ecologically valid conditions. Similar challenges have been noted in other complex socio-technical systems, where relying on formal models alone falls short without empirical insight into how users perceive risk and make decisions in close-to-realistic contexts (Cheng et al., 2025). For example, in a security context, a self-reported approach, in which users report their security concerns, may be subject to a phenomenon similar to the "privacy paradox," in which people report strong privacy concerns, but in practice behave in a privacy risky way (Barnes, 2006; Norberg et al., 2007). In previous studies, other layers were added, to enrich the self-reported data, and their authors designed experiments to elicit users' security and privacy (S & P) decision-making. For example, researchers designed experiments using conjoint analysis methodology (Frimpong and Helleringer, 2021; Ayalon et al., 2023), and, in a stream of studies, used a behavioral economics framework (Tsai et al., 2011; Redmiles et al., 2018; Acquisti et al., 2013), with some specifically using auctions (Danezis et al., 2005; Li et al., 2021).

In this study, we also used a methodology that is based on behavioral economics principles to understand users' security decision-making. We expand prior security knowledge by exploring it in a *digital account valuation* context, linking security choices with valuation considerations. As previously suggested (Herley, 2009) and empirically explored (Redmiles et al., 2018), users have cost-benefit considerations when making security decisions. Here, we utilize users' valuations of their digital accounts to gain insight into security-related decisions. That is, what aspects of their accounts are considered when deciding whether to behave more or less securely? Prior S & P work explored the value of specific information types, such as location (Danezis et al., 2005), or within a given account (Bauer et al., 2012).

We follow prior work, where researchers aimed to understand users' valuations of their digital accounts by using a scenario in which users were prevented from *accessing* their accounts (Corrigan et al., 2018; Mosquera et al., 2020). We took a security perspective and investigated users' reaction to the possibility that their accounts would be *compromised*. Thus, we learned about their security considerations regarding the protection of an account as a whole and the way in which their threat models are related to their account valuation and willingness to allow an account to be compromised.

In a different study, the authors assumed that users would assign different values to different types of accounts, and that their security behavior, specifically password creation, would differ accordingly (Ur et al., 2015). Here, we go beyond this assumption and design a study that allows us to witness users' valuations of different types of accounts in practice and how these valuations relate to their security decision-making. Such a methodological approach enabled us to understand various aspects naturally considered by users (i.e., without being asked about specific security mechanisms, for example), including the type of information and how the account is used or connected to other accounts. To that end, our paper answers the following research question: *What factors drive people's decisions to explicitly give away access to their accounts and data?*

To answer this question, we used second-price auction experiments with 66 participants at two university campuses, where participants competed to perform a risky behavior task: In exchange for money, they would give us their account credentials, which would then be published on the darknet. Following experimental (Redmiles et al., 2018) and theoretical (Solove, 2021; Nissenbaum, 2004) security and privacy studies, the authors of which posit that security decision making is context-dependent, we explored four types of accounts: email, social media, online-offline (e.g., Uber), and news. We took a qualitative approach to examine participants' security decision-making in our account valuation settings. Following the experiments, we interviewed the participants who won the auctions ($n = 21$) and conducted focus-group discussions with those who chose to participate in the auctions (i.e., decided to bid), but did not win ($n = 27$).

Following prior auction-based valuation work, we use the bidding mechanism as a way to elicit how participants reason about their accounts when incentivized to engage in an insecure action (Huberman et al., 2005). By attaching monetary incentives to a security-compromising decision, the auction serves as a proxy for real-world pressures, such as convenience, time constraints, or desire to continue using a

service, that might shape security behavior in practice (Petrykina et al., 2021). Our analysis focuses on the *relative differences* in bidding behavior, and the qualitative rationales participants provide, using bids as a lens to surface salient considerations (e.g., data sensitivity, account utility, and perceived threats), rather than as estimates of stable account value.

Our findings show that most participants (73%) were willing to *bid on at least one of their accounts and provide us with their credentials.* Furthermore, a significant minority (29%) was willing to do so on what we considered a sensitive account type—their *email* account. However, while this might initially be regarded as highly insecure behavior, our post-experiment discussions revealed complex security decision-making on the part of many of the participants. For example, participants considered *account characteristics*, such as whether it was their primary or secondary account when they had multiple accounts with the same service provider.

In this study, we focus on understanding the considerations that shape users' security-related decisions. In addition, our work has secondary economic relevance. Specifically, we report the monetary amounts participants were willing to accept in this experimental setting as a means of contextualizing relative differences across account types and decision rationales, rather than as estimates of underlying or stable account value. As suggested by prior work (Frik and Gaudeul, 2020), such relative measures may still be informative for policy discussions. We do however caution against interpreting bids as direct proxies for how users value their accounts outside the experimental context, particularly given strategic bidding behavior and varying levels of engagement with the compromise scenario.

Beyond security-related findings discussions, we also discuss the study methodological aspects, including strengths and limitations. Our study design helps bridge the gap between what is understood about the factors affecting account valuation and the role of context for critical security decision-making. Although we aimed our methodology to be ecologically valid by creating a realistic scenario, achieving full ecological realism in security studies is inherently challenging. For example, Fahl et al. (2013) found that approximately 30% of participants showed no resemblance between study passwords and their real-world passwords, based on a categorization of password similarity. More broadly, this tension between ecological realism and experimental control is well documented in auction-based valuation research on digital services and personal data. Such studies commonly rely on academic settings and incentive-compatible designs to elicit willingness-to-accept under perceived costs, rather than to reproduce literal real-world behavior (e.g., Danezis et al., 2005; Corrigan et al., 2018).

Some of the challenges we encountered that threatened ecological validity included participant recruitment, the academic nature of the study, and ethical considerations. We elaborate on these in §5.4 and §5.5. Despite these limitations, the self-reported findings from our participants are relevant for uncovering key important factors and their complex and contextual interaction that govern the account valuation, as similarly demonstrated in prior auction-based valuation studies conducted under comparable constraints (Danezis et al., 2005; Corrigan et al., 2018).

Ultimately, we discuss our findings in light of S & P theoretical background, particularly the context-dependent nature of decision-making (Nissenbaum, 2004). We suggest strategies to encourage security-preserving behavior while accounting for users' tendency to make decisions based on context, and explore ways to highlight the perceived value of their digital accounts. Broadly, our contributions are as follows: (*a*) *We conducted the first in-laboratory auction study for account types other than social media and the first study on account compromise versus loss of access.* (*b*) *Our experiment proxied insecure decision-making to offer an in situ perspective on people's justifications for insecure behavior.*

2. Related work

Our work contributes to the literature on security and privacy (S & P) decision making and valuation. In the following, we review behavioral economics studies on assessing users' digital accounts and personal information valuation and prior work on S & P decision making.

2.1. Measuring the value of free-access goods

Economists in general estimate consumer surplus to measure the value of free or low-cost goods and services (Brynjolfsson et al., 2003; Ghose et al., 2006; Bapna et al., 2008; Greenstein and McDevitt, 2011). Consumer surplus is the difference between the highest price people are willing to pay for the goods and the actual price they pay. Instead of assessing people's willingness to pay for goods and services to which access is free, economists elicit the value people are willing to accept to forgo these goods. In these willingness-to-accept studies, researchers examined the monetary valuation of Facebook, in particular (Corrigan et al., 2018; Mosquera et al., 2020; Allcott et al., 2020), and to a lesser extent other online platforms such as Google (Herzog, 2018), and considered the way the valuations are related to individuals' well-being (Brynjolfsson et al., 2019), consumer welfare (Corrigan et al., 2018; Allcott et al., 2020), users' ability to detect biased news headlines (Mosquera et al., 2020), and other intangibles, such as political polarization (Allcott et al., 2020). However, allowing access to an account is only one aspect of account valuation. We leveraged the same methods to explore our participants' reasoning about account valuation in the context of security by measuring the amount of money they would accept in exchange for allowing another party to access their accounts.

2.2. Monetary value of personal information

Over the years, researchers have studied in diverse contexts the value people place on various types of personal data, such as location (Danezis et al., 2005; Cvrcek et al., 2006), finances (Hann et al., 2007; Carrascal et al., 2013), personally identifiable information (Acquisti et al., 2013; Hirschprung et al., 2016), and information associated with digital accounts (Bauer et al., 2012; Ur et al., 2015; Spiekermann and Korunovska, 2017). Our study operationalized their valuation of personal information by asking people to place bids on accounts that are used to create, store, and share different types of personal information. In prior studies, auction-based methods were used to elicit users' monetary valuations of personal information and digital services, including non-hypothetical settings with binding consequences at the time of the study (Corrigan et al., 2018; Huberman et al., 2005). These studies, along with those conducted using discrete-choice experiments (Brynjolfsson et al., 2019; Prince and Wallsten, 2022), showed that the users' actual value of personal data varies by data type, and that determining an absolute value to summarize users' valuations could lead to inconclusive results. Our study was thus focused on understanding the factors that affect people's valuation of digital accounts, both individually and together, and unraveled the different perspectives of people on the same type of information. Unlike most previous studies that asked participants how much they valued limiting their own account use (Corrigan et al., 2018; Mosquera et al., 2020; Brynjolfsson et al., 2019), our study asked them to allow access to their accounts—which they might not be able to take back—making our findings more consequential.

2.3. Security and privacy decision making

The results of prior studies suggest that S & P decision making is highly contextual (Nissenbaum, 2004; Acquisti et al., 2015). Researchers explored specific populations, such as refugees in the US (Simko et al., 2018) and people from Kenya (Munyendo et al., 2023), revealing the manner in which the environment influences peoples' security behavior. In both these studies, users heavily relied on managers (managers of cybercafes in Kenya and case managers in the US) to conduct computer-mediated tasks, even to the extent of allowing them to select and manage their passwords (Munyendo et al., 2023). Recent work has also found that the adoption of security behaviors is costly in terms of time and convenience, that people have a limited "compliance budget" (Beautement et al., 2008) to spend on such costs, and that these costs may deter people from adopting security behaviors (Redmiles et al., 2018; Morrison et al., 2021; Murray and Malone, 2023; Kautondokwa et al., 2021).

In our opinion, this study provides a bridge covering the gap between what factors people consider in their account valuation and what they prioritize when making S & P decisions. It is difficult to protect all the accounts and data an individual might own. Nevertheless, security researchers can review

our work to understand what is most important to people and thus can design improved measures to protect them.

3. Methods

We conducted a laboratory experiment to determine which factors render people's digital accounts valuable to them. To ensure the accuracy of our findings, it was necessary that our participants believed they would be giving away their account credentials. Thus, we used Vickrey auctions with reserve prices as our primary method to elicit participants' valuation of their accounts, followed by an online survey to gather more knowledge. The participants who bid and won the auctions then participated in further discussions in focus groups or individual interviews with the researchers. These participants are the primary focus of this paper. Our institution's ethical review board (No. 22-06-3) authorized the study and it was conducted between July and November 2022.

3.1. Eliciting security and privacy decision-making

There are multiple established approaches for eliciting S & P decision-making. Prior work has used stated-preference methods such as conjoint analysis (Frimpong and Helleringer, 2021; Ayalon et al., 2023) and discrete choice experiments (Molin et al., 2018) to study tradeoffs among predefined attributes (e.g., privacy properties, incentives, or system features), as well as behavioral economics approaches that elicit decisions under incentives or perceived risk (Tsai et al., 2011; Redmiles et al., 2018; Acquisti et al., 2013), including auction-based mechanisms (Danezis et al., 2005; Li et al., 2021). These approaches differ in the extent to which the decision space is specified by the researcher versus shaped by participants' own reasoning. Conjoint analysis and discrete choice experiments are well suited for estimating the effects of researcher-defined attributes in structured choice settings (Hainmueller et al., 2014). However, this reliance on ex ante specification makes such methods less suitable for exploratory settings aimed at eliciting which considerations users themselves find salient.

In contrast, our study seeks to elicit how participants reason about the value and protection of their digital accounts in a holistic and context-dependent manner, without constraining them to a predefined set of security or privacy factors. To support the spontaneous emergence of participants' own considerations, we adopt an incentive-compatible behavioral economics approach based on auctions, which ties decisions to perceived consequences rather than to predefined attributes. Here, we used Vickrey auctions, which are sealed-bid, second-price auctions (Vickrey, 1961), in which participants place bids to purchase goods (or a service). The participant with the highest bid wins the auction and pays for the goods at a price equal to the second-highest bid. The mechanism is designed to be *incentive-compatible*, as it is in all participants' best interest to bid their true value of the payment to maximize their utility rather than under- or over-bidding (Vickrey, 1961; Hurwicz, 1972; Lucking-Reiley, 2000). As in prior work where the Vickrey auction was used to measure people's value of digital services (Danezis et al., 2005; Corrigan et al., 2018), in our experiment, winners bid the lowest compensation and received the second-lowest requested amount in the auction. Furthermore, our auction included a *reserve price* (Ausubel and Cramton, 1999), which allowed us to set an upper limit on the price the winners would receive. The reserve price was unknown to the bidders, but they were informed of its existence.

3.2. Participant recruitment

We recruited the participants between July and November 2022 through advertisements sent to email lists and printed flyers. The study was conducted at universities in two cities in Germany, and the recruitment differed according to the location. To recruit participants in Kaiserslautern, we used the university's newsletter. To recruit participants in Saarbrücken, we used (*i*) department and social emailing lists and (*ii*) physical flyers and digital advertisements posted on notice boards and handed out to people at cafeterias. More effort, and therefore the use of more recruitment channels, was needed to recruit participants in Saarbrücken, since recruitment took place also during the summer vacation and thus students were less available. Ultimately, we recruited 34 participants in Kaiserslautern and 32 in

Saarbrücken. Since the study was conducted at university locations, most participants were students, and some had a background in computer science ($n = 7$).

Participants first completed an online screening survey, using *Qualtrics* (Qualtrics, 2020) (see §A for the survey). The purpose of the screening was to identify participants who owned at least one digital account that was at least one month old in each of these categories: Email, Social Media, and Online-Offline (such as a food-delivery application, in which the order is performed online and the user receives the food offline). The requirement that the participants had owned their account for at least one month was intended to increase the probability that they would consider their account to be valuable, at least to some extent, as compared to an account they had recently created, following the methodology of prior economics studies (Brynjolfsson et al., 2023) with the same methodology. In addition, the survey also examined whether the participants had an optional account in the News category, although this did not affect their eligibility. Our initial motivation for including news accounts was to serve as a low-stakes comparison point: we hypothesized that users would generally perceive news accounts as less sensitive and therefore be more willing to bid on them. However, as we observed that ownership of such accounts was relatively uncommon, and given the already limited recruitment pool, we chose to treat news accounts as optional rather than as a requirement for participation.

For each account category, the survey presented to the participants a list of online services and asked them to select accounts at least one month old. The order of the presented lists and the items within the lists were randomized. The lists were drawn from the Alexa top 100 and further filtered based on the popularity and availability of the services in the country where the experiment was conducted; the lists were validated and revised using a pilot survey.

Across both locations, 298 people filled our screening survey. Of these, 205 were eligible, i.e., had owned at least one account for at least a month in each of the three mandatory account categories mentioned above. We asked these eligible participants to provide their email addresses for follow-up communication and redirected them to *Setmore*, a scheduling service, to state their availability for the study. As expected, some of those who registered did not come to the experiment. In B, 32 individuals out of 79 who registered participated (41%), and in A, 34 individuals out of 55 participated (62%). One explanation for the higher attendance rate in A might be the recruitment timing, as mentioned earlier.

3.3. Experiment design

We designed and deployed a within-subject user study to understand the way users determine the valuation of their digital accounts. To design the study, we closely followed Corrigan et al.'s (2018) methodology, including using their training materials that they shared with us. Our user study consisted of four parts (see Figure 1). (i) **Training**: We explained to the participants the operation of the Vickrey auctions with reserve price and gave them multiple examples, together with a hypothetical auction. Then, (ii), they participated in the real **Account Auctions**. In this part, participants were told the auction was "real," and that if their bids won, they would receive the winning amount in exchange for their account credentials. Next, (iii), they completed a **Demographic Survey** that collected their demographics and other auction-related details while the researchers ran the auctions. Finally, (iv), we revealed to the participants the **Auction Results** and the next stages based on the results: (a) completion of an *online survey*, if they chose not to bid in (ii); (b) participation in a *focus group*, if they chose

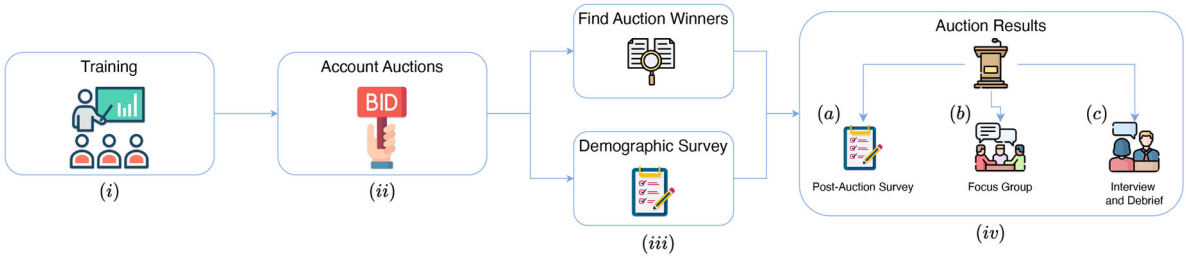

Figure 1. Experiment design and all the four stages, as described in §3.3.

to bid but did not win; or (c) an *interview* with the researcher if they won the auction and thus were willing to give their account credentials. We describe each of these parts of the experiment below.

i. **Training.** When participants arrived for the laboratory study, we (the researchers) registered them. After all the participants for the session had arrived, we handed them a printed survey that included a consent form and the first two parts of the experiment: Vickery auctions explanation and training, as well as the actual account auctions. Throughout the experiment, the participants had the printed survey in front of them, while we used a presentation to help participants follow the explanations easily.
Participants were explained about the three possible compensation levels, based on the stage the participant would reach. *Stage* (a) : Completion of an online survey, € 15; *Stage* (b) : Participation in a focus group, € 12.5 per hour; and *Stage* (c) : Participation in an interview. For *Stage* (c), we explained that they would be paid € 12.5 per hour and any additional payment based on their bids. During the **Training**, we told the participants they would be bidding to perform a task. We explained the exact task details in the second part, **Account Auctions**.
We then used the printed survey and the presentation to walk the participants through the details of the auction process with the help of examples. The primary purpose of these examples was to ensure the participants understood the process of the second-price Vickrey auctions (Vickrey, 1961) with reserve price and test their understanding. Since our auctions considered willingness-to-accept, we illustrated the bidding process using a hypothetical example in the survey, using the same scenario and explanations as used by Corrigan et al. (2018). We asked the participants the minimum amount they would bid to sell us their shoes. To test the participants' understanding, the survey asked them four questions. Three questions included an example of auctions with illustrative players bidding different amounts, borrowed from Corrigan et al. (2018). The survey asked participants to indicate which illustrative player they thought would win and the amount of money they thought the winning player would be paid. The fourth question was the same as the previous three, but introduced the participants to the existence of a reserve price (see Figure 2). The reserve price allowed the maximum compensation amount we would pay a winner to be set. To win, the bidders also had to bid less than the reserve price, but they never knew its true amount. The answers to all these questions were used only to train the participants, and their answers here did not affect their participation or compensation.

ii. **Account Auctions.** After reminding them briefly about the auction process, we told the participants that the bids they would write in the following set of questions would be their real bids and, if they won, they would need to perform the task. Next, we described "the task" as bidding on giving us their account username and password, one in each account category—email, social media, online-offline, and news (if they had one). We instructed them that they should not change these for a week if they chose to give us their account credentials. We would verify whether the credentials were correct, and the winners would have to turn off any additional security login measures,

Figure 2. Example of a question from the training phase, as discussed in §3.3. Question asked: "accordingly, what if charlie bids €325, deborah bids €0, edward bids "No", and the reserve price is €225? Who would give us the shoes? How much she or he would be paid?" the correct answer is deborah, and she would receive 225 euros.

Table 1. Participant demographics.

Demographic	Category	%age	*n*
Gender	Female	45.45%	30
	Male	50.00%	33
	Non-Binary	3.03%	2
	No Answer	1.52%	1
Age	$18-25$	31.82%	21
	$26-35$	62.12%	41
	>36	6.06%	4
Education	Attended/Completed Graduate	24.24%	16
	Attended/Completed Undergraduate	64.12%	41
	High School or Below	13.64%	9

such as two-factor authentication. We added that we would post these account credentials on a darknet hacker forum, and the participants should assume their accounts would be hacked.

However, in reality, we never accessed or saw the participants' account usernames or passwords. The task was a necessary deception to ensure the experiment's success.

So that our experiment would be tied to seemingly real consequences, we needed participants to believe that their bids would truly amount to the risk of losing their account credentials, as has been done in past research (e.g., Danezis et al., 2005; Corrigan et al., 2018). We reminded the participants before the actual task that they could withdraw if they wished. The participants who won the auctions and successfully finished the task were debriefed about the study goal during *Stage* (c).

When the participants had learned the complete process, the final step was to bid in the real auctions. Based on the screening survey, we prepared the printed survey with the selected online services for each category. If a participant selected more than one account in a category, we randomly selected one. The participants were asked to bid on three or four accounts (if they had a news account). We told them the minimum bid amount could be €0 and there was no limit on the maximum bid amount, but that they should keep the existence of a reserve price in mind. We also told them they could choose the 'No Bid' option. The participants individually wrote their bids on their printed surveys. The order of the accounts was randomized.

iii. **Demographic Survey.** After the auction, we instructed all participants to complete an online survey. We used this survey to collect participants' demographics, as detailed in Table 1. We utilized this time to collect the printed surveys and calculate which participants had won the auction. We input the participants' bids from the printed surveys to a Python program we created to output the auction winners for each category and the next stages for all the participants.

iv. **Auction Results.** Based on the auction results, we assigned the participants to one of the three final *stages* described earlier. *Stage* (a) : If they did not bid on any of the accounts, we instructed them to fill an online post-auction survey about their decisions during the experiment. *Stage* (b) : If they bid on their accounts but did not win the auction, we assigned them to a focus group discussion consisting of up to eight participants, following focus group's methodology best practices (Krueger, 2014). *Stage* (c) : If the participants won the auction for any of their accounts, they were chosen to perform the task and participate in a one-on-one interview with the researcher. We reminded *Stage* (c) participants that they would have to give us the username and password of the account for which they placed the winning bid.

To elaborate, the winner for each auction by account type was led to a private room with a computer to perform the task individually, in the presence of only the auction winner and a researcher. We showed the participants how to blur the computer screen to protect their privacy during the experiment. We falsely added to our explanation that the computer was running software to record their credentials when they had logged in. This deception allowed them to believe they were actually giving away their account credentials, while in reality, the process was completely private. After they had blurred the screen, keeping only their profile name visible, the researcher could verify that the credentials were valid. This completed the final stage of the experiment. Next, we debriefed the participants who completed this final step about the study and explained that we do not have any key-logging software, and thus, their credentials were not recorded. During the debriefing, we explained why the

deception was necessary to obtain the true valuation of the accounts and that they had to believe their bids were tied to real outcomes in conjunction with the auctions. We discuss the interesting results related to participant trust in the experiment setup in §4.1 and the ethical considerations in §5.6. We asked a limited number of participants if they believed our deception, since we had concerns about information spread among potential participants as the experiment was conducted over a couple of weeks at two campuses (see §5.5 for limitations). We also asked the participants not to disclose the study procedure to others to minimize demand characteristics (Rosenthal et al., 2009). Then, we asked them to log out and described the best practices for creating a strong password, and interviewed them about the process.

The interview was designed to (1) help us understand the participants' decision-making throughout the study, (2) learn about their thoughts on the auction process, and (3) learn about their thoughts on the actual task of giving us their credentials and the consequences of this action. The focus group protocol and the questions in the post-auction survey were for the most part identical to the interview protocol. We customized the language based on whether the participants won the auction or not, but the topics were similar. We list the complete protocols in §B.

3.4. Analysis

The interviews and the focus group discussions were audio-recorded by the researchers and transcribed by a transcription service. Using thematic analysis, two researchers then analyzed the interview data, taking a hybrid approach (Fereday and Muir-Cochrane, 2006). The researchers discussed the initial set of codes and independently coded four interviews and focus group discussions, from both A and B participants. The researchers then discussed their findings and developed themes beyond the initial codes, and updated the codebook and the previously coded interviews. The researchers repeated the process to code two additional transcripts individually and discussed updates in the codebook. Using the codebook developed from this process (provided in §C with definitions), the researchers independently analyzed a total of 19 interviews and 9 focus groups.

3.4.1. News account

While news accounts were owned by a smaller subset of participants (n = 17), we retained them in the analysis. Although their lower representation limits quantitative comparison across account types, participants' decisions regarding news accounts, such as refraining bidding, provided useful qualitative insight into how users reason about accounts they perceive as low sensitivity or low value. Accordingly, we use news accounts primarily to examine participants' reasoning in low-perceived-stakes contexts, and interpret findings related to these accounts with appropriate caution.

4. Results

In this section, we first present the descriptive statistics of the participants' decisions. We then focus on our qualitative analysis of the interviews and focus group discussions that highlight the contextual factors that determine account valuation.

Table 2. Statistics of participant bids by account types. All bid amounts are in euros (EUR, €). the minimum and the mode for each account type was 0. *News* accounts were owned by a subset of participants (n = 17) and are included mainly for descriptive purposes.

Account type	Mean	Std. Error	Med.	Max	Bidders (%)
Email	867.4	570.6	20	10K	19 (29%)
Social	145.2	47.3	10	1K	32 (48%)
Online-Offline	284.2	139.0	12	5K	37 (56%)
News	9.4	6.3	0	69	11 (65%)

4.1. Descriptive statistics

We present the bid amounts for each account type in Table 2, together with the number of participants who chose to bid. The participants who did not bid on their accounts valued them too highly to give their credentials away. The mean bidding amount for email accounts was € 867.4, with a median of € 20. It is important to note that, of 66 participants, only 19 (29%) chose to bid on their email accounts, which was *the lowest percentage of bidders among all the account types*. Then, online-offline accounts' mean bid amount was € 284.2 and median bid amount was € 12 placed by 37 participants (56%). Social media accounts' mean bid amount was € 145.2 and median bid amount was € 10 placed by 32 participants (48%). Among participants who owned a news account (n = 17), a majority chose to bid on it, resulting in a mean bid amount of € 9.4 and a median of € 0 (65% bidders). Given the lower ownership rate of news accounts, these figures are reported descriptively and are primarily used to contextualize bidding behavior in low-perceived-stakes settings.

4.2. Qualitative results

Our qualitative analysis highlights the factors that influenced the participants' decision to bid or not to bid on their accounts and, by extension, the factors that govern their valuations. In general, our findings can be categorized into four main topics: *Trust in the Experiment*, *Data and Privacy Beliefs*, *Possible Threats*, and *Account Properties and Utility*.

Participants expressed their *Trust in the Experiment* and referred to aspects such as the extent to which the researchers were convincing and the experiment location (academic institute). *Data and Privacy Beliefs* factors were related to the participants' beliefs about the sensitivity and availability of their data, as well as to their beliefs about the importance (or lack thereof) of those data remaining private. Next, participants' mental models of the *Possible Threats* influenced their bidding decisions. For example, participants referred to threats such as data misuse and financial risk. Participants also mentioned topics that were in general related to *Account Properties and Utility*, such as the connections between their accounts, having multiple accounts on the same platform, and the frequency of their account use.

4.3. Trust in the experiment

Participants' decision to bid was sometimes related to the experimental context. For example, participants' motivations included curiosity, desire to gain knowledge, and willingness to win the game. Participants also responded to our questions about the effect of the experimental setting on their decisions.

A total of 12 participants expressed curiosity, willingness to learn about cyber security, and excitement. Participants explained they decided to bid because they were curious about the study and wanted to see the outcome. While referring to curiosity as a reason to bid, in their detailed response, participants also considered the specific account on which they decided to bid, as explained by P23:

> Yeah, I definitely had concerns for Gmail and Discord. So, I did not even go there. Like I did not want to risk it. For Tier [scooter-sharing], I had some concerns. But I also was curious about the whole process. So, I was like, let's go for it.

Nineteen participants explained that they set a low bid amount because they wanted to win the auction. The participants understood that, to win, they would need to bid a low amount, and that was part of their considerations, as explained by P12, referring to bidding on her *Discord* (an instant-messaging social) account:

> For me, the strategy was clear, just bid the lowest. We did the examples. The lowest always wins, so why not just use zero?

Interestingly, participants who explicitly cited winning as a motivating factor also articulated account-specific reasons for their bidding decisions, which were similar to those cited by participants who did not mention winning as a motivation (see §4.4.5 for an example).

Some participants, from both focus groups and personal interviews, were asked whether the location of the experiment, an academic institute, affected their bidding decisions. Most of them ($n = 17$) said it had an effect, and a few said it had not ($n = 5$). The academic context made participants feel safe and think that providing their credentials would not be too harmful to them. Nevertheless, they expressed "calculated risk," referring to accounts that did not include personal data. Those who were not affected by the academic context explained that they took the task seriously, as they assumed that the account would be hacked, as expressed by P14:

> I was pretty serious. I thought that my account was going to be shared. […] And I was just sharing some accounts where I do not have much information.

Winning participants were asked several questions to help us understand whether the experimental settings affected their bidding decisions. Seventeen participants were asked whether they believed we would indeed publish their credentials. Nine participants answered that they did, and eight participants answered that they did not. Those who believed we would publish, explained that the researchers were convincing and that the additional request to blur the screen made the situation seem real. Other participants, such as P3, thought that we, the researchers, *"are not really going to sell it online to some guy on the black market."* Further analysis comparing the believing and non-believing participants did not reveal any significant differences in account categories, and both groups stated reasons to bid related to their privacy beliefs, account properties, and perceived threats, detailed in the following sections.

4.4. Data and privacy beliefs

Participants referred to their beliefs about various aspects of the data as reasons for deciding whether to bid or not or to set the bid amount. For example, participants referred to the data's level of privacy, availability, and type, such as location or pictures. In the following, we present examples of these and other topics mentioned in the participant discussions. We show examples of the discussed topics as well as the varying decision directions (e.g., mentioning privacy considerations as a reason both to bid and not to bid).

4.4.1. Data sensitivity

Cumulatively, 21 participants out of 66 referred to data sensitivity, *i.e.,* the extent to which their data are private and/or sensitive. Closely related to this, fewer participants ($n = 13$) referred to the importance of the data. The participants also referred to specific data types and the associated threat of exposing those data. In particular, participants explained their decision whether to bid while referring to specific data types such as location, photos, and emails. Participants also raised concerns (or non-concerns) about the data availability—the degree to which they perceived the data to be public, and volume—the amount of data that could be exposed.

Exemplifying data importance, participants discussed the importance of data in their email accounts. P3 explained he used his *Gmail* for both personal and professional communication, and this was the reason he chose not to bid on it:

> Because it's super important, all the information I get from my job, from my university. Then like personal stuff, […] Like my mom sending me an email with important information.

In other cases, participants referred to the age of the data within it as a reason to bid on the account, as expressed by P9. However, similarly to other data attributes, where one person might refer to the age of the data as a reason to bid, other people might consider the old data to be of nostalgic value, as we later discuss in §4.3. Here, P9 explains why she chose to bid on one of her email accounts:

> Yes, for the Hotmail account, I bidded [sic] because I'm now using more Gmail than Hotmail. In Hotmail, there are old emails, not the new ones.

Participants mentioned the volume of the data that might be exposed if their accounts were compromised and its effect on their decision to bid. As we discuss below in 4.4.1, some participants had multiple accounts on the same platform. Some used this mechanism to limit the amount of personal information they divulged to third-party services and attenuate the risk of losing the account. P11

explained to us that he set up his *secondary* email account to accomplish this protective strategy, such that a low volume of data was exposed:

> Some websites, you go to log in and they ask you to give your email ID, so I had just one account created which I use for all of those stuff. So, I was bidding on this account because I know that it doesn't have any of my personal information.

An additional instance of a low data volume being at risk referred to social media accounts. In this case, the volume is determined by the way in which the account is used. Among our participants, 10 mentioned that they used their accounts only to consume content, and hence, did not post any valuable information. P25 bid on her *Twitter* account and said the following as one of the reasons for her decision:

> I am mostly like a content consumer instead of a content creator. So, there is also like maybe two, three, four tweets that I have in this account.

4.4.2. Data type

Location data were one example of the way the perceived data-sensitivity varied and the possible exposure of their data influenced participants' decisions. Participants talked about location data when they were asked about their online-offline and social accounts. We show the different perspectives on location data in the following examples. P1 chose not to bid on his *Facebook* account and mentioned the amount of data social media accounts collect over time, including location. He explained his reason for choosing not to bid:

> … Facebook has most of my personal data, my conversations and my details like friends and location history or the apps that I connected with Facebook. So that's why I didn't provided [sic] it.

Conversely, a different participant (P2) shared her reason for deciding to bid on her *Lieferando* account, a food delivery application in Germany, explaining that the location data saved in her account were easily accessible:

> … I think the only identifiable thing there is my address, and this is kind of quite easy to get. I think it's not so valuable to me.

4.4.3. Privacy attitudes

While participants were not directly asked about their general privacy attitudes, a few participants (P10, P29, P24) expressed low privacy concerns. Using Westin's Privacy Index (Kumaraguru and Cranor, 2005), these participants expressed attitudes that place them in the group of people with the lowest level of concern (out of three possible levels): "Privacy Unconcerned." In the experiment context, these low-level concerns led them to bid on their accounts with a low value. For example, P10 bid on all of his accounts (email, social media, and online-offline) and explained:

> I have nothing to hide, and I was [not worried about] information might get leak[ed]. So nothing to worry about. So zero for all.

In addition to making bidding decisions based on their own privacy concerns, a minority of participants ($n = 2$) considered privacy risk to others in their valuations. For example, when asked why she chose to bid € 300 on her *Twitter* account, P25 explained that compromising her account could lead to the exposure of her friends' private information:

> … I'm not giving the password for zero euros [because] this account is following so many of my friends, which their Twitter accounts are private. So maybe their data, their information is also going to be affected by my account.

4.5. Possible threats

Throughout the discussions, we learned about participants' mental models of the threats they might encounter if their credentials were publicly shared. In addition to referring to threats, such as misuse of

personal information ($n = 15$) and reputation harm ($n = 6$), participants also mentioned possible unforeseen threats as a result of their lack of awareness of what their account might include. Our finding that connects participants' mental model possible threats to their bidding decision is supported in prior work. For example, referring to people who experienced suspicious login incidents, it was found that people's mental models of the attacker influenced the actions they took to protect their accounts (Redmiles, 2019).

4.5.1. Data misuse

We asked the participants what they thought might happen when their accounts were compromised. A common threat model that participants ($n = 15$) conceived was the misuse of personal information. Three participants mentioned that their personal data might be sold for money and subsequently could be used for tracking and targeting them when the account was compromised. In addition, six other participants alluded to the possibility of malicious actors using their personal data to learn about their behavior and analyze their habits. Data misuse was mainly mentioned as a reason not to bid. Only two participants referred to this topic as a reason to bid, either considering the possible consequences as minor or doubting that the hackers could in fact analyze their data. P4 was among the participants who bid on her *Lieferando* account and explained the way in which her data could be used to track her habits:

> I could guess they can just see how often I order something and what are my habits, if they have any other data that will link it to it and see why I decided to do that. At the end, they just want to sell you more things.

In another example, P2 considered the ways in which her *Instagram* photos could be misused. She explained she was aware a bad actor could misuse her photos, but she was not worried about this and chose to bid € 1000 on her account. P2 was confident that the misuse of her photos would not cause her significant harm in the short term, but that still did not mean she wanted to give her information for free:

> I don't really care if they [pictures] are out there. [This is] how I feel now, I don't know how I'll feel in 50 years […] as long as my head is not photoshopped onto some weird pictures […] I don't think they can be used against me. […] But then I bid on it, because I don't want to give it away for free.

4.5.2. Financial risk

Financial risk was another threat that the participants raised when considering what would happen after the bidding. This was in particular relevant in the context of online-offline accounts. Specifically, participants ($n = 3$) said they chose to bid a high amount that was determined by the amount of money that could be withdrawn using their accounts. For example, P3 considered the financial loss he would sustain after bidding on his *Tier* account:

> I thought about how much it would impact me financially if one person would be able to scoot around for one week […] Let's say 1000 euros makes sense. So even if they drive like every day, full time, I'd still be able to pay that after the seven days where I could change my password.

Similarly, a discussion during the focus group led P18 to mention he would bid an amount on his *Lieferando* account that was higher than the anticipated amount for a food order so that he could be compensated for the loss.

Participants also mentioned the way they could reduce financial losses through the security measures of payment services. Some participants ($n = 3$) mentioned that the authentication step required by *PayPal* before the final payment made them feel more secure. For example, P6 considered this extra security step as a part of the reason for bidding on his online-offline account:

> I have to believe [in PayPal] with their basic security. When you say you want to order something, and if you want to pay with PayPal, which I always try to use, it will be redirected to my PayPal application, and from there, I have to agree and put my PayPal password or my fingerprint, one of them.

Another participant, P16, who bid on her *Lieferando* account, told about her practice of using *privacy.com* for online purchases. The website allows her to mask the actual credit card number by means of the provision of virtual credit cards that could be canceled at any time:

> So with the Lieferando account, I felt really secure in that if it did get compromised, my credit card information isn't going to get taken by anybody because [… privacy.com is basically…] like a PayPal but it just gives you a fake credit card number to make purchases through and everything goes through them but with a third-party buffer.

4.5.3. Data loss

Participants referred to the possibility that they would lose access to their account. Such a risk not only exposes user data to malicious actors but also prevents the users from accessing their own data. One category in which this issue was particularly salient was the social media accounts. Accounts such as *Instagram* allow users to create a digital archive of their major life events and share it with their friends and family. Some participants expressed that these data are of high value to them. As we mentioned in §4.2, that the data in an account were old did not necessarily mean the participants were willing to bid on that account. P4 elaborated on her choice of not bidding on her *Instagram* account she has had for 11 years. The fear of losing access to her account played a significant role in her decision:

> . . There's a lot of pictures, kind of chronological timeline of my life. … It's a lot of pictures that are not harmful if they are exposed, but I would not want a hacker deleting them… It's like my online album. … And so, I value that aspect of it.

4.5.4. Social harm

When considering how a compromised account could be used to inflict damage, the participants ($n = 6$) mentioned the potential reputation harm as one factor that governed their bidding decision. P21 said he placed a high bid on his News account because of his concerns about the possible damage to his reputation:

> I bid 100 euros on speaking on the news because of their appeal. You also got more opportunities to misuse the name by doing nonsense comments which I basically sent with my name.

In a similar vein, participants were more likely to bid on an account if the probability that doing so might cause reputation damage was low. For example, P14 decided to bid on his *Twitch* account, a live streaming platform for gamers, since his account was anonymous and therefore bore no risk for reputation damage or social harm:

> "I have no followers, nothing. No one knows that I am on Twitch… It's anonymous identity for me"

One of the participants (P24) also expressed trust in his social connections who would negate any possible harm due to anomalous posting behavior on his *YouTube* account. He bid €0 on his account and explained why he was not concerned:

> … the worst thing that could happen is people create some disturbing video using my account [YouTube]. But I trust the people around me and know they won't believe any such thing.

An additional common mechanism that could be employed by an attacker to cause social harm is the scamming of an account holder's friends and family, and the participants ($n = 7$) echoed this concern. For example, P5 said:

> So, the hackers would go to the messenger and pose as me and ask my friends for money. And I don't want that stuff to happen…

4.5.5. Data unawareness

During the focus groups, five participants who chose not to bid expressed concerns about their incomplete awareness of their account content and the information that could potentially be exposed. This unawareness of the nature and the amount of data present in their account and the threat of the data being misused could hinder the participants' estimation of the risk. For example, P4 decided not to bid on her *Gmail* account. Here, as was expressed in other participants' discussions, the correlation between account age and data unawareness is clear:

> Any other accounts, like my Gmail, I've been using it also for a long time. So, there might be a lot of data saved on those accounts that I don't remember right now. But I prefer not to take that risk.

4.6. Account properties and utility

In their discussions about whether to bid, participants referred to several factors that were directly related to the discussed account. In general, we noticed that some of the factors were personal and related to the perceived utility of the account, such as, their frequency of use. Other factors were more architecture-related. For example, participants considered whether an account was a "stand-alone" one vs. one connected to other accounts. We describe the factors arising from the account connections as network effects and further divide them into *explicit network effects*, *i.e.,* when the network created by the service provider, and *implicit network effects*, *i.e.,* when the network created by the user.

4.6.1. Multiple accounts

It is now easy to create more than one account on the same platform. In our study, 21 participants acknowledged having more than one account on the same platform. Some of the reasons mentioned were that they used the different accounts for different purposes—limiting access to personal information ($n = 5$) when signing up for a new service and differentiating personal and professional communications ($n = 9$).

One of the participants, P3, owned two *Facebook* accounts, and he specifically bid € 10 on the older one and not on the one he created recently when he started his studies at the university. As inferred from his explanation, beyond the data that the new account contains, it has a higher utility since it enables him to create and maintain connections with people from the university and outside, thus making it more valuable than the older account.

> For Facebook, I had to choose 10 euros, because I couldn't care about the account, and I don't think anyone else would care. I have that account since I'm like 13. […] For University, I made a new Facebook account, which was really plain, really simple and only has one picture. It has real important friends or people I know from university. Unlike the old account is like a 14 to 15-year-old kid used to have. So, I don't see any value in that.

In addition to social media accounts, participants also mentioned having multiple email accounts on the same platform. For example, P1 bid on one of his two *Gmail* accounts:

> This is a secondary account I have, […] and I can provide you with this account since I don't have more privacy issues in this particular account.

Having more than one account is a low-cost measure that allows participants not only to secure their data and access other online services but also to marginalize account valuation and limit risks.

4.6.2. Interchangeable accounts

In addition to reporting having multiple accounts on the same platform, the participants also reported on the way accounts on different platforms can be used for similar purposes, making them interchangeable in some cases. This was prevalent in the case of accounts that depend less on user data and more on providing a real-life service, such as food delivery or scooter-sharing accounts. A total of 11 participants mentioned the ease of replacing an account as one factor determining its valuation. P14 bid on his *Tier* account, and his decision was motivated by the ease of switching to another account:

> I don't care really about [Tier]. I can go onto some other transport service and I can start using that.

Online-offline accounts rely less heavily on user data and account usage to provide an acceptable user experience than email and social media accounts. However, some services employ user retention strategies, such as loyalty benefits that are tightly coupled with the account, reducing the interchangeability. Four participants expressed concerns over losing such loyalty benefits if they lost their accounts. P2 summarized it:

> So, if [my Lieferando] got hacked and I lost my points, then I would be annoyed.

4.6.3. Explicit network effects

We define *explicit* network effects as cross-account dependencies that arise from deliberate user actions that link multiple accounts. In these cases, users actively create or configure connections between accounts, often to improve convenience or usability, but in doing so introduce cascading security risks. If one account is compromised, access to other linked accounts may also be affected. Participants described several types of explicit network effects. These included using Single Sign-On (SSO) for signing up ($n = 7$), connecting online-offline accounts to payment services ($n = 21$), using email accounts for password recovery ($n = 2$), and using the same password for multiple accounts ($n = 4$). In all such cases, obtaining user credentials for an account can affect others.

SSO (Sun et al., 2011; Wang et al., 2012) is an authentication method that allows users to use an existing account (e.g., Facebook, Google, Apple) to sign up for a new service without registering a new username and password. It facilitates the user's account creation and alleviates the need to remember an additional set of credentials. Conversely, if an SSO account is lost, in addition to the account itself, all the connected accounts are also lost. P15 understood this risk and elaborated on his decision not to bid on his *Facebook* account:

> Well, because also nowadays, you enter other websites, they will say sign in with Facebook, sign in with Google, or some of my websites are signed in by Facebook. If I give one of the Facebook account[s], that means the others are given away.

Participants also mentioned payment services as an additional means of connecting digital accounts. In addition to the traditional payment methods (e.g., cash, credit, or debit cards), online payment services such as *PayPal* and *Venmo* have become extremely popular (F.I. Services, n.d.). This is especially common in the case of online-offline accounts, which allow users to link an account to an external payment service for easy payment. The connection had different effects on the participants' bidding decisions. For example, P18 bid € 100 on his *Lieferando*, which was influenced by the amount of money in his *PayPal* account. He explained:

> … I chose to sell it for 100 euros, because I thought that it's maybe connected to my PayPal account. So, if somebody hacks it, how much will they order? Maybe they order food on my name, so they maybe order food for 56 euros. So, if I get 100 euros, I'm somehow compensated.

Conversely, another participant (P12) exemplified risk aversion concerning financial loss and did not bid on his *Lieferando* account. He explained his discomfort with the connection to *PayPal*:

> And my Lieferando is connected to my PayPal. I mean, I still need to log in every time in my PayPal, but I don't feel comfortable people even being able to have access to something where I buy stuff. So that's why I didn't provide this information

Similarly, the participants who had not linked their accounts to any payment service were more likely to bid on their accounts. P29 bid on his *Lieferando* account citing this reason:

> And even if I am hacked, my payment details are not mentioned there. So I thought that maybe it's not a big deal even if I'm hacked or something.

An additional connection that affected participants' bidding decisions was the use of email accounts for password recovery mechanisms. Email accounts allow users to add an additional email to recover forgotten passwords. P6 took this connection into account and chose not to bid on his *Gmail* account:

> All of [the accounts] are connected somehow because, let's say I disconnected with another account and that account, if someone tries to log in, maybe send a verification here or something like that.

Four participants stated that they used the same password for multiple accounts. In our study, we allowed the participants to change the password for the account on which they were bidding before they gave it to us. Two participants told us they were concerned about changing their passwords before bidding because they had a common password for these accounts. The other two participants said they had the same passwords for accounts they considered unimportant. P2 explained:

> But I have like categories of passwords for like not so important websites. So, I use the same password for those. And then for the important like Instagram and stuff, I use kind of a similar password.

In such cases, losing the username and password for one of those accounts could expose the others as well.

4.6.4. Implicit network effects

In contrast, we define *implicit* network effects as cross-account dependencies that are imposed by service providers, rather than created by user choice. These effects arise from platform architectures in which multiple services are accessed through a single underlying account or credential, limiting users' ability to disentangle or selectively protect individual services. This was prevalent in the case of *Google* accounts, which are implicitly dependent on each other. *Google* owns many online services such as *YouTube* and *Gmail*, all of which are accessed by the same account. Therefore, when bidding on one of these accounts, the participants had to bid on the common account, the *Google* account. Thus, when bidding on this account, the participants would be giving away the credential for multiple accounts "for the price of one."

In the case of some participants ($n = 18$), their selected social media account was *YouTube*; however, since *YouTube* uses the same *Google* account as the *Gmail* account, the participants ($n = 5$) considered the network effect between the account on which they were bidding and the other accounts that would also be compromised by this decision. One of the participants (P9) explained her action of placing a high bid (€ 500) on her *YouTube* account:

> I bidded [sic] in a higher price because if you have access to my YouTube account, you will have access to all the Google services.

Similarly, in a focus group discussion, P18 elaborated his reasons for not bidding on his *Gmail* account:

> I did not bid on Gmail, because it's linked to many different accounts like Google Drive and many other things.

Although the participants had no control over these implicit network effects of *Google* accounts, they were aware of it and used it as a factor for their account valuation.

4.6.5. Frequency of use

One of the core factors affecting the participants' valuation of their accounts was the amount they used them. Naturally, the frequency of account use had an inverse relationship with the likelihood of participants bidding on the accounts. A total of 15 participants referred to their low use of the account as a reason to bid or bid a lower amount. For example, P2 said the following about her bid of € 100 on her *Lieferando*.

> I placed kind of a low amount on it because I don't really use it that much.

Conversely, one participant, P12, explicitly said that she uses her *Gmail* account very frequently and for this reason she did not bid on the account:

> … I send emails almost on a daily basis, maybe every two, maybe every few three days. … So that's why I didn't provide this information.

Furthermore, frequency of account use spanned across participants who mentioned winning the auction as a motivation and those who did not (described in §4.1). P29, who mentioned winning the auction as a motivation, and P30, who did not, both bid € 0 on their *Hotmail* accounts specified one of the reasons was because they rarely used it. The frequency of account use is one of the direct utilities for the participants, and the more they used the account, the more valuable it was to them.

5. Discussion

In this study, we examine how users reason about security-related decisions involving their digital accounts, using account valuation as a lens to surface the considerations shaping those decisions. We conducted a behavioral economics study with 66 participants, measuring participants' willingness-to-accept payment for providing their digital accounts' usernames and passwords. The primary results in

the current paper are based on the qualitative analyses of discussions with selected participants ($n = 48$) who reached the focus group or interview stage. While we found evidence of a meaningful influence of the account type on the particpants' account valuation, as hypothesized, other context-related factors, such as beliefs about the data associated with the account and the account properties, also play a significant role. Our results support the findings of prior studies and highlight the contextual nature of security decision making. We discuss our observations in the light of the results of prior studies and suggest implications for future security design and research.

5.1. Theoretical implications

The results of prior theoretical and empirical studies suggest that security and privacy decision making is context-dependent (Acquisti et al., 2018; Solove, 2021; Nissenbaum, 2004). Similarly, we hypothesized that users' willingness to protect different types of accounts would differ, since in general they represent different "context-relative informational norms" (Nissenbaum, 2009). Participants gave varying explanations for their decision whether to bid, with the type of the account being one of them. However, their explanations were far more nuanced than that, revealing other factors taken into consideration. We found that participants referred to four broad topics: Trust in the Experiment, Data and Privacy Beliefs, Possible Threats, and Account Properties and Utility. Some of the factors related to data beliefs and possible threats are highly aligned with Nissenbaum's contextual privacy model (Nissenbaum, 2009). For example, the model's parameters include "attribute" (type of information), and "actors" (data subject, sender, recipient). Factors influencing participants' decisions during the experiment included *attribute-related* aspects, such as the sensitivity and importance of the data contained in the account. Similar results were observed in prior work, where data sensitivity influenced users' security behavior, such as deciding to anonymize their identity (Huberman et al., 2005; Peddinti et al., 2014). Participants also referred to the type of the data (e.g., location and photos) and its content, e.g., *"Like my mom sending me an email with important information"* (P3). These results support early work that highlighted the role of context in how it affected users' valuation of data (Danezis et al., 2005; Carrascal et al., 2013) (i.e., users' movements influenced their location data value). Through participants' mental models of possible threats, we observe considerations that are *actors-related*. For example, participants considered potential misuse of their data, such as it being sold and subsequently used to target them.

Beyond factors related to Nissenbaum's contextual privacy theory, users revealed other influential factors. For example, participants considered the *account* characteristics and the possible consequences of the account being compromised. The discussed account might be linked to other accounts through, for example, corporation ties, i.e., *YouTube* and *Gmail*, both of which are *Google* services, or through password recovery email.

We observed contextual decision-making, in which participants referred to *common topics* but based their decisions on their *personal situation*. The same topic was discussed as a reason for both bidding or not bidding, for example, with participants explaining that they have or do not have privacy concerns related to a discussed account. Our findings provide an initial framework for exploring the factors that influence account-related security behavior. We highlight the complexity of this decision-making process, which involves multiple context-dependent considerations.

5.2. Gaps in security decision-making

We took a cost-benefit approach in our study, which was previously used to explore users' security decision-making. For example, several papers aimed to explore security mechanisms in a given context, in which participants considered the cost of behaving more securely (e.g., Redmiles et al., 2018; Beautement et al., 2008; Morrison et al., 2021; Murray and Malone, 2023). In these papers, we learned about some of the factors that influence users' security decisions, such as increased cognitive load (Beautement et al., 2008) or expected risk (Redmiles et al., 2018). In our study, participants were presented with a task that resulted in users' security considerations—some of them similar to those reported in prior work (e.g., data sensitivity and importance), and some were either not or rarely

reported in a security context (e.g., primary vs. secondary account). Here, we aggregate the factors observed in our study and put our results in conversation with prior work.

5.2.1. Data and privacy beliefs

As referred in 5.1, we support prior work, finding that users considered the data type and sensitivity in their security decision-making. Privacy beliefs influenced some of our participants' decisions as well. Prior work, however, showed that general privacy attitudes either had a small or no effect (Huberman et al., 2005; Spiekermann and Korunovska, 2017).

5.2.2. Possible threats

Participants referred to several types of threats that influenced their decisions, such as data misuse or finance-related threats. Different types of risks were previously reported, with results depending on the explored variable and study context. For example, the severity of possible risk did not significantly influence users' intent to behave securely in one study (Kautondokwa et al., 2021), but explicitly stating the risk to the users was the most influential factor in another (Redmiles et al., 2018). Finance-related risks were reported in prior work as reasons to behave securely (Prince and Wallsten, 2022; Abraham et al., 2021). Interestingly, participants in our study referred to the risk of losing their data, which was rarely mentioned in prior work. For example, exploring older adults, participants were concerned they might lose their data if they use security measures incorrectly (Morrison et al., 2021). Our participants, however, were concerned they might lose data as a result of others *gaining access* to their account, thus able to decide which data to delete. This finding points to a factor that studies might often overlook as a possible outcome of a poor security behavior.

5.2.3. Account Properties and Utility

In their explanations, participants referred to several aspects related to the account, including how it is used by them and connected to other accounts. Users previously referred to the connection between their email and other accounts through account recovery (Ur et al., 2015; Abraham et al., 2021). Interestingly, in prior work from 2015 (Ur et al., 2015), many users perceived different types of web sites as of similar value: news site, a banking site, and an email account. In the study from 2015, only few participants mentioned email account as one that can be used as a recovery account. Therefore, our results highlight the shift in users' perceived differences between the accounts' values, and as a result, the necessity to secure them differently.

Our participants brought other considerations that were account-specified, referring to whether the account was primary or secondary (e.g., more than one Gmail account), or whether it was easily interchangeable (e.g., in which participants did not care whether they would use a specific platform to order food, for example). These considerations were not reported before in the context of security behavior, to the best of our knowledge. In the context of privacy, multiple account usage has been reported in studies of teenagers, for example, who use several accounts to keep their privacy from their parents (Page et al., 2022). Our results highlight the role of multiple accounts also in the context of security behavior, beyond privacy. Lastly, participants referred to their use of the account, which was previously reported in cost-related security study (Bauer et al., 2012). The study, from 2011, found that users' valuation of their data on Facebook was related to how they used Facebook (i.e., diary keeping), but not to how much they used it. While our study is qualitative and therefore not comparable, we learned that participants considered their use of the account in their decision. Here, too, our results may point to the shift in users' perceptions and consideration over time.

In sum, our work enriches the literature on users' security decision-making in several ways. Findings-wise, we support some of the factors reported previously (data sensitivity consideration), and in other cases, we point to possible shifts in users' perceptions (account use frequency). In other cases, we find factors that were rarely considered before, such as accounts hierarchy within the same service provider (i.e., primary and secondary Gmail accounts). Methodologically, we employ a distinct approach compared to prior cost-benefit security studies, yielding new findings. While our study design allowed participants to set their own value, prior work set it experimentally (Redmiles et al., 2018). The

context in our study was digital accounts, whereas in prior work the context was more specific, such as information type (Danezis et al., 2005) or a specific account, such as Facebook (Bauer et al., 2012). Lastly, our study is unique in its in-situ exploration of the connection between account valuation and security behavior (i.e, deciding whether to give away access to one's account).

5.3. Research and design implications

5.3.1. Raising awareness of account value

Prior work has shown that security awareness is a critical predictor of protective behavior (Al-Balushi et al., 2024; Huang et al., 2011), and several interventions have sought to raise users' awareness of security risks (Albayram et al., 2017; Scholefield and Shepherd, 2019). Building on this general understanding, we highlight an additional and often overlooked perspective: users' awareness of account value. While users take cost–benefit considerations into account when deciding whether to behave in a security-protective way (Duggan et al., 2012; Redmiles et al., 2018; Herley, 2009; Beautement et al., 2008; Morrison et al., 2021; Murray and Malone, 2023; Kautondokwa et al., 2021; Fagan and Khan, 2016; Florêncio et al., 2014; Beautement and Sasse, 2009; Spiekermann et al., 2012), we find that people may easily forget the value of their account over time, or they may not consider the account sufficiently valuable to warrant protection in the first place. Regarding the latter, participants mentioned in several contexts their lack of awareness or knowledge about the content of the account on which they were bidding. Participants were unsure whether other accounts were linked to the discussed account or what data it might contain. This lack of awareness was mentioned mostly in the context of old accounts, either those that had been used for a long time or those that had not been used for a while. This finding supports prior work showing that people consider data importance and sensitivity in their privacy and security decision making (Peddinti et al., 2014; Abraham et al., 2021), as well as the account connectivity (Abraham et al., 2021).

From a security perspective, being more aware of the account content is beneficial in several ways. For example, users might want to consider deleting underutilized accounts. Eliminating such accounts would help them reduce security risks and vulnerabilities while enabling higher productivity (Khan et al., 2021; Uğur and Alışkan, 2022; Sweeten et al., 2018). Prior work has shown undeleted "zombie" accounts could be inherited by new users unwittingly (Liu et al., 2022). In addition, targeting users who are unaware of their account contents or linked accounts, can help them surface the privacy and security risks that are not immediately obvious and potentially adopt better security practices.

As we observed in many cases, knowing they had sensitive data in their accounts gave people a sufficient reason not to bid on them. A possible design direction can aim to increase users' awareness of their account's content, both the data and the accounts linked to it. The latter has been explored in depth by Hammann et al. (2022). They interviewed lab participants to uncover the *account access graphs* and found that the participants had an incomplete view of their online account setup and reused passwords for unimportant accounts. Interestingly, these findings appear naturally in our study (see §4.4.3) and reinforce the relationship between user awareness and better security practices. To investigate this direction further, future work can lean on prior work in which S & P-oriented visualization strategies (Hammann et al., 2022; Takano et al., 2014; Angulo et al., 2015) and digital data management tools were explored (Khan et al., 2021).

5.3.2. Using contextual security

In our study, we explored accounts' valuation through security decision-making. We found that participants' valuation varied across *contexts*: participants were willing to provide us with their account credentials depending on different factors they took into account (such as possible information misuse or whether the account was a primary or secondary account). While considering both various angles of security decision-making—where some study authors ask whether people should invest effort in security behavior (e.g., Redmiles et al., 2018; Herley, 2009)—and our work exploring accounts' valuation through a willingness to protect them, similar conclusions can be drawn: People's security behavior depends on their current security-related situation (Redmiles et al., 2018; Hammann et al., 2022). Relatedly, work on decision-making in complex systems has explored how users adapt strategies under

uncertainty, providing a broader theoretical backdrop for considering how future security systems might reason about strategic user actions and contextual factors at scale (Cheng et al., 2025; Cheng et al., 2025).

As we observed, some accounts are simply of low value to users, *i.e.,* they contain no data or were possibly coerced into creation by the service provider (e.g., news websites, shopping websites). Considering contextual security, as security researchers, we can use people's observed tendency to secure those accounts that they consider valuable and encourage them to secure also accounts they might consider of less value but are in fact valuable. Thus, we join the users in conducting "contextual security," helping them with highlighting contexts, or risks, they might miss. As proposed in previous papers (Redmiles et al., 2018; Herley, 2009), it may be sensible to wait until an account has gained value before users are prompted to secure that account *or* it may be the case that users should be able to negotiate lower security requirements for accounts of low value that have no interconnection with more valuable accounts.

5.3.3. Security in practice

Taken together, our findings suggest two complementary directions for translating account valuation into practical security support. These directions point toward future technologies that assist users without imposing uniform or overly prescriptive security requirements.

5.3.3.1. Value visualization. Drawing on nudging theory (Thaler and Sunstein, 2009), and in the context of security and privacy in particular (Acquisti et al., 2018), one practical direction is to increase users' awareness of account value through visualization. Such an approach offers a way to surface information that is often difficult to grasp, such as an account's accumulated or long-term content, in a manner that supports users' decision-making without restricting their choices. Future systems could explore visual representations that make otherwise implicit aspects of account value explicit. This may include visualizing features that participants identified as meaningful, such as the types of data associated with an account (e.g., financial data) or the extent to which an account is connected to others. Importantly, such visualizations need not prescribe specific actions; rather, consistent with nudging approaches, they can shape the choice architecture by making value and risk more salient at moments when users are already engaging with security-related decisions. Designing effective value visualizations raises open research questions regarding what information should be surfaced, how it should be aggregated, and how to balance informativeness with cognitive load, making this an important direction for future work.

5.3.3.2. Understanding users' context, and helping users understand the context. A second, complementary direction concerns the use of context-aware security support. Prior work on context-adaptive privacy (Schaub et al., 2015) emphasizes that privacy and security regulation is dynamic and situational, rather than static. Our findings similarly suggest that participants' security decisions were shaped both by who they were as users and by the specific account and situation under consideration. Specifically, we suggest three design directions.

5.3.3.3. Modeling user context. From a user-centered perspective, future systems may seek to model aspects of users' security and privacy orientations, for example, based on prior security behaviors or stated preferences (Di Ruscio et al., 2024). Such models could inform adaptive defaults or recommendations, allowing systems to tailor security support to different users rather than adopting a one-size-fits-all approach. For example, to prompt less security-savvy users only when security risks are extremely high.

5.3.3.4. Modeling account and situational context. At the same time, context also arises from the technology itself. Accounts differ substantially in their role within users' digital lives, for instance, in whether they function as primary accounts, are used frequently, or contain sensitive data. Future systems could leverage such signals to contextualize security interventions. For example, when prompting

a user to change a password, the system could adapt the framing and urgency of the prompt based on whether the account serves as a central identity provider or contains high-impact information, as opposed to a low-use or peripheral account.

5.3.3.5. Contextualizing decisions through awareness. Consistent with prior work on situational privacy awareness (Schaub et al., 2015), such context-aware mechanisms could also help users better understand why a security action is recommended. Making contextual factors explicit, such as visualizing that an account is frequently used, linked to other services, or stores financial data, can support users' decision-making by aligning security recommendations with their existing mental models. Rather than issuing generic prompts, systems can thus encourage proportionate security actions that reflect both the user's orientation and the account's situational context.

5.4. Methodological implications

Here, we discuss several methodological considerations that inform how the results of this study, particularly bidding behavior, should be interpreted and considered in future work using similar methodologies.

5.4.1. Incentive compatibility

Participants explicitly referred to their willingness to win the game and the way it motivated them to bid zero on their accounts. Such decisions raise interpretive questions about whether participants genuinely valued their accounts at zero. Although Vickrey auctions are incentive-compatible, there may be alternative explanations for participants' bidding behavior—particularly in cases where zero bids were submitted. Prior research on strategy-proof mechanisms has shown that individuals do not always act in accordance with their true preferences. For instance, in the context of school matching, Hassidim et al. (2017) suggest that participants may misreport preferences due to mistrust in the system or the belief that their true choices will not be seriously considered. Similarly, some of our participants stated that they did not believe we would actually disclose their credentials.

Focusing on Vickrey auctions, Sandholm (2000) outlines several well-documented limitations that lead to untruthful bidding. For example, he notes the complexity involved in computing one's bidding value and how, in practice, this value may need to be approximated. In our experiment, which incorporated a reserve price component in addition to the standard Vickrey auction structure, participants may have been distracted by the experimental setting itself. This may have led them to bid zero strategically to win the game, possibly without fully considering the risks. However, referencing both possible explanations—bidding complexity and disbelief in the setup—we observed that participants appeared to engage in "calculated risk," placing low bids specifically on accounts they were less concerned about, as discussed in §4.1 & §4.4.5.

In addition to understanding people's privacy and security considerations, data valuation estimates are important from an economic perspective as well. They provide useful input for assessing financial penalties in case of a data breach (Li et al., 2021) and help policymakers design evidence-based privacy regulations (Frik and Gaudeul, 2020). Li et al. (2021) support the viability of using an auction-based approach to measure the value of personal information, and Tan et al. (2018) found that although the absolute valuations are context-sensitive, the relative valuations remain stable across contexts. However, while previous work discusses the potential real-world applications of these numerical values, we suggest they should be interpreted with caution. As discussed, there may be alternative explanations for low bids—such as zero—beyond truly assigning no value to the account. Accordingly, our findings should be interpreted as illuminating how users reason about account value and security tradeoffs under perceived risk, rather than as estimates of stable or context-independent monetary valuations.

5.4.2. Experimental realism

Prior work has emphasized the importance of realism when studying the factors that affect how people value digital goods and services (Tan et al., 2018). At the same time, we note that achieving full ecological realism in security and privacy research is inherently challenging. In our study, the semi-realistic

setting nevertheless enabled participants to articulate detailed explanations for their bidding decisions, many of which were grounded in account-specific considerations rather than the experimental context itself.

In particular, the academic environment in which the study was conducted emerged as a salient factor shaping perceived risk and trust. As reported in Section 4.1, many participants explicitly stated that the university setting and their trust in the researchers reduced their perceived likelihood of harm and increased their willingness to bid. While this context enabled participants to engage with a sensitive security scenario in an ethically appropriate and controlled manner, it also represents a central limitation: observed bidding behavior may partially reflect institutional trust effects rather than account valuation alone. In nonacademic or industry contexts, such as interactions with commercial services or third-party intermediaries, participants may reason differently about risk, potentially placing greater emphasis on worst-case outcomes or declining to engage altogether. Future work could explore these differences by varying institutional cues, employing third-party intermediaries, or conducting field studies outside academic environments.

5.5. Limitations and future work

In our auctions, we asked the participants to bid on *one account* in each category, stating that the winner would reveal the username and password for *one account*. However, there were two scenarios where participants eventually could only bid on more than one category or had the choice of bidding on one of many in the same category. In one scenario, the randomly selected account comprised more than one account owned by a single entity. For example, when participants were bidding for their *YouTube* credentials, they would essentially be bidding on their *Google* account, which would also be their *Gmail and Google Photos* account. Similarly, there also existed a network effect for SSO accounts (§4.4.3). For example, a participant (P9) mentioned that she logged in to her *Tier* account via her *Google* account. In this scenario, even if our study protocol allowed users to change the password for the account on which they were bidding, we could not disentangle the perceived valuation of this account from that of the connected account.

In a different scenario, people bid on accounts other than their primary ones (§4.4.1). Participants were asked to bid on one randomly selected account within each category; when they held multiple accounts for the same service, we limited them to a specific one. We did not explicitly require participants to identify or bid on a "primary" account in advance, which allowed us to observe how different aspects of an account factored into participants' valuation and security reasoning. As a result, participants were often more relaxed about bidding on accounts they considered secondary, which in turn surfaced how users reason about various account's aspects, such as its interchangeability, centrality, and perceived replaceability. While these scenarios might be considered limiting from a strictly controlled comparison perspective, our qualitative study revealed decision-making factors, including distinctions between primary and secondary accounts, that may have remained less visible had participants been restricted to bidding only on primary accounts. Future work could explicitly control for or manipulate account selection to examine how such distinctions interact with account type and valuation outcomes.

In our study, we attempted to create a realistic scenario for the participants such that they would truly believe they were bidding on giving away their account credentials. However, the physical environment of university locations carried limitations in that it emphasized the credibility of the experiment and some participants' decisions could have been influenced by the apparent safety a research study may provide. Eight out of seventeen participants who were asked if they believed we would actually disclose their credentials answered "no" after they were debriefed. To protect the integrity of the ongoing experiment, we only asked this of the participants who made it to the interview stage. Nevertheless, even among those who expressed disbelief, many articulated deliberate, account-specific reasoning, suggesting that bidding decisions reflected valuation factors rather than belief in the literal execution of the compromise scenario. For example, when asked P10 said he believed the compromise scenario, while P1 said he did not. They both bid on their *Gmail* accounts and shared common factors like "this is a secondary account I have" (P1) and "there's nothing personal information stored in that" (P10).

Our results summarize the key factors that shape participants' valuation of their accounts. As discussed above, they are best interpreted as reflecting participants' reasoning rather than precise monetary estimates. We observed general trends in some cases, such as participants who feared data loss for their primary social accounts and did not to bid on them. However, other relationships were more complex and hard to generalize. For example, participants' beliefs about the sensitivity of location data varied: some considered aggregated location data on *Facebook* as more sensitive, while others considered food-delivery location data as less sensitive. This complexity highlights the need for further quantitative research to explore the effect of the identified factors on user valuation and, in turn, on security decision-making.

Our study included four account types: three mandatory categories (email, social media, and online–offline accounts) and one optional category (news). Additional account types, such as banking, healthcare, or government accounts, were considered but ultimately excluded due to both practical and regulatory constraints. In particular, in the German context, strong authentication requirements (e.g., mandatory two-factor authentication for online banking) prevented us from asking participants to disable protections or grant access in a manner consistent with our study protocol. Moreover, to keep the study design relatively simple and feasible for participants, we intentionally limited the number of account types included. While participants frequently discussed financial risk and sensitive data in relation to the accounts studied, the inclusion of additional high-stakes or institutionally regulated accounts could surface different considerations or emphasize certain factors (e.g., data type, legal implications) more strongly. Examining how account valuation and security reasoning extend to such accounts remains an important direction for future work.

Our population sample consisted primarily of young, educated participants, recruited at university campuses in Germany, which may limit the generalizability of our findings to broader or more diverse populations. In particular, account valuations and security decision-making may differ across age groups, professional backgrounds, and cultural contexts. Prior work suggests that such differences are not merely theoretical: studies on sociodemographics and security behavior show that age, education, and digital skills are associated with distinct security perceptions and practices (Wei et al., 2024), and, for example, research on older adults indicates higher concern about online risks alongside lower adoption of certain protective mechanisms and limited awareness of recovery or reporting options (Pacheco, 2024). While our study reveals important decision-making principles within our examined population, future work should examine whether these patterns hold in more diverse and cross-cultural samples.

The study was conducted in 2022, which is approximately three years before the time of publication. Although the data has aged since collection, we believe it is still valid. For example, in a different study, a one-year difference did not significantly change people's privacy behaviors and perceptions (Redmiles et al., 2019). Also, considering the COVID − 19 pandemic, when people's perceptions might have differed from "usual" times, the data was collected toward the end of the pandemic.

Future work can explore the impact of selected factors on security behavior or on the way users perceive their digital account's value. One direction would be to explore ways to increase users' awareness of their account content, such as reminding them of old data whose existence in the account they might have forgotten. Possibly, reminding them of such data would encourage them to protect their account better. A different direction would be to explore users' account valuations while considering the network effect (either through single entity accounts or SSO) and people's primary accounts. Such a study could reveal whether the proportions found in our study, e.g., the percentage of people willing to bid on their account per type, may differ in a further study.

Our study relied on a deception-based scenario that framed account access as being posted on a darknet marketplace in order to elicit realistic security decision-making. While this framing was effective in prompting participants to reason about risks, threats, and consequences, future work could systematically examine how different levels or forms of realism influence users' responses. For example, alternative designs could vary the framing of access (e.g., full credential disclosure, temporary access tokens, or partial account lockout) to assess whether similar valuation factors and decision-making themes emerge without extreme or highly evocative narratives. Such work would help disentangle the role of framing from underlying security reasoning and further refine experimental methods for studying sensitive security behaviors.

5.6. Ethical considerations

One serious challenge in privacy and security research is measuring people's true perceptions, as participants' responses are often shaped by hypothetical framing. To address this challenge, prior S & P research has employed highly realistic study designs, including, in some cases, deception, to elicit meaningful valuation behavior and decision-making (Distler et al., 2021; Cranor and Buchler, 2014). Such work includes studies that relied on real and binding disclosure of personal information (Huberman et al., 2005), as well as studies demonstrating that realistic framing, sometimes involving deception, can materially affect valuation outcomes even when no actual disclosure occurs (Tan et al., 2018). In our study, exposing participants' actual account credentials would pose unacceptable security and legal risks. We therefore adopted a realistic but hypothetical scenario, using deception as a more conservative alternative to real disclosure while preserving methodological realism. Specifically, we designed the experiment to convince participants that, when they bid on providing us with their digital account credentials, those credentials would be made available to hackers.

During the bidding sessions, some participants asked questions that indicated their consideration of potentially stressful implications, such as giving hackers access to connected financial accounts. Beyond these questions, we did not encounter any behavior indicating stress, and participants freely exercised their autonomy in choosing whether to bid on conducting the task. Participants who falsely believed they had given us their credentials were immediately debriefed. We clarified that the entire story was a deception and that we never intended to collect participants' credentials or post them on hacker forums. We explained that the deception was used to understand digital account valuation in a close-to-real context.

Additional ethical steps were taken. Before conducting our study, we obtained approval from our institution's Ethical Review Board (ERB). Participants provided informed consent prior to participation. The study was conducted in person, and demographic data were collected, including age, gender, and education level. Because participants identified themselves in person, we assigned randomly generated IDs and separated identifiable information (e.g., names and email addresses) from the collected data.

In summary, we explicitly considered potential ethical concerns related to perceived coercion, participant distress, and deception in the study design. Participation was fully voluntary, and compensation was used as part of an incentive-compatible design to elicit meaningful decision-making; participants were informed that outcomes could differ based on their choices, retained full autonomy to bid or decline, and were never required to disclose real credentials or take irreversible actions in practice.

Acknowledgment

The study was conducted when most authors were affiliated with the Max Planck Institute for Software Systems in Germany. Elissa M. Redmiles was a group leader, Oshrat Ayalon was a postdoc, and Shubham Singh and Jackie Hu were interns. We would like to thank the institute for its significant support in conducting the study.

Author contributions

CRediT: **Shubham Singh**: Data curation, Formal analysis, Investigation, Project administration, Software, Visualization, Writing – original draft, Writing – review & editing; **Jackie Hu**: Writing – original draft, Writing – review & editing; **Cormac Herley**: Conceptualization, Methodology, Writing – review & editing; **Elissa M. Redmiles**: Conceptualization, Funding acquisition, Methodology, Project administration, Resources, Supervision, Validation, Writing – original draft, Writing – review & editing; **Siddharth Suri**: Conceptualization, Methodology, Writing – review & editing; **Oshrat Ayalon**: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Use of Generative AI

We confirm that we used Generative AI tools (ChatGPT v5 and v4o) for text rephrasing, conceptual brainstorming, code assistance, and literature search (via Undermind.ai). These tools were used to support language clarity, facilitate idea development, and identify relevant literature.

ORCID

Shubham Singh http://orcid.org/0000-0003-1540-8511
Oshrat Ayalon http://orcid.org/0000-0002-5905-9838

References

Abraham, M., Crabb, M., & Radomirovíc, S. (2021). *I'm Doing the Best I Can." Understanding technology literate older adults' account management strategies* [Paper presentation]. International workshop on socio-technical aspects in security (pp. 86–107). Springer. https://doi.org/10.1007/978-3-031-10183-0_5

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). *Privacy and human behavior in the age of information*. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274. https://doi.org/10.1086/671754

Al-Balushi, A., Tarhini, A., Acikgoz, F., & Ali, S. (2024). Examining the factors that influence user information security behavior toward covid-19 scams. *International Journal of Human–Computer Interaction*, *40*(24), 8809–8826. https://doi.org/10.1080/10447318.2023.2291608

Albayram, Y., Khan, M. M. H., & Fagan, M. (2017). A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *International Journal of Human–Computer Interaction*, *33*(11), 927–942. https://doi.org/10.1080/10447318.2017.1306765

Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2020). The welfare effects of social media. *American Economic Review*, *110*(3), 629–676. https://doi.org/10.1257/aer.20190658

Angulo, J., Fischer-Hübner, S., Pulls, T., & Wästlund, E. (2015). *Usable transparency with the data track: a tool for visualizing data disclosures* [Paper presentation]. Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (pp. 1803–1808). https://doi.org/10.1145/2702613.2732701

Ausubel, L. M., & Cramton, P. (1999). *Vickrey auctions with reserve pricing*. Papers of Peter Cramton.

Ayalon, O., Turjeman, D., & Redmiles, E. M. (2023). *Exploring privacy and incentives considerations in adoption of COVID-19 contact tracing apps* [Paper presentation]. 32nd USENIX Security Symposium (USENIX Security 23) (pp. 517–534).

Bapna, R., Jank, W., & Shmueli, G. (2008). Consumer surplus in online auctions. *Information Systems Research*, *19*(4), 400–416. https://doi.org/10.1287/isre.1080.0173

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

Bauer, C., Korunovska, J., & Spiekermann, S. (2012). *On the value of information-what facebook users are willing to pay* [Paper presentation]. ECIS 2012 Proceedings.

Beautement, A., & Sasse, A. (2009). The economics of user effort in information security. *Computer Fraud & Security*, *2009*(10), 8–12. https://doi.org/10.1016/S1361-3723(09)70127-7

Beautement, A., Sasse, M. A., & Wonham, M. (2008). *The compliance budget: Managing security behaviour in organisations* [Paper presentation]. Proceedings of the 2008 new security paradigms workshop (pp. 47–58). https://doi.org/10.1145/1595676.1595684

Brynjolfsson, E., Collis, A., & Eggers, F. (2019). Using massive online choice experiments to measure changes in well-being. *Proceedings of the National Academy of Sciences of the United States of America*, *116*(15), 7250–7255. https://doi.org/10.1073/pnas.1815663116

Brynjolfsson, E., Garro, H., Collis, A., Deisenroth, D., Liaqat, A., Wernerfelt, N., Kutzman, D., & Lee, J. J. (2023). *The digital welfare of nations: New measures of welfare gains and inequality*.

Brynjolfsson, E., Hu, Y., & Smith, M. D. (2003). Consumer surplus in the digital economy: Estimating the value of increased product variety at online booksellers. *Management Science*, *49*(11), 1580–1596. https://doi.org/10.1287/mnsc.49.11.1580.20580

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. (2013). *Your browsing behavior for a big mac: Economics of personal information online* [Paper presentation]. Proceedings of the 22nd International Conference on World Wide Web. ACM. https://dl.acm.org/doi/10.1145/2488388.2488406

Cheng, L., Li, M., Tan, C., Huang, P., Zhang, M., & Sun, R. (2025). Computational game-theoretic models for adaptive urban energy systems: A comprehensive review of algorithms, strategies, and engineering applications. *Archives of Computational Methods in Engineering*, 1–78. https://doi.org/10.1007/s11831-025-10364-y

Cheng, L., Yu, F., Huang, P., Liu, G., Zhang, M., & Sun, R. (2025). Game-theoretic evolution in renewable energy systems: Advancing sustainable energy management and decision optimization in decentralized power markets. *Renewable and Sustainable Energy Reviews*, *217*(C), 115776. https://doi.org/10.1016/j.rser.2025.115776

Corrigan, J. R., Alhabash, S., Rousu, M., & Cash, S. B. (2018). How much is social media worth? estimating the value of facebook by paying users to stop using it. *PloS One*, *13*(12), e0207101. https://doi.org/10.1371/journal.pone.0207101

Cranor, L. F., & Buchler, N. (2014). Better together: Usability and security go hand in hand. *IEEE Security & Privacy*, *12*(6), 89–93. https://doi.org/10.1109/MSP.2014.109

Cvrcek, D., Kumpost, M., Matyas, V., & Danezis, G. (2006). *A study on the value of location privacy* [Paper presentation]. Proceedings of the 5th ACM Workshop on Privacy in Electronic Society. ACM. https://doi.org/10.1145/1179601.1179621

Danezis, G., Lewis, S., & Anderson, R. J. (2005). How much is location privacy worth?. In *WEIS* (Vol. 5). Citeseer.

Di Ruscio, D., Inverardi, P., Migliarini, P., & Nguyen, P. T. (2024). Leveraging privacy profiles to empower users in the digital society. *Automated Software Engineering*, *31*(1), 16. https://doi.org/10.1007/s10515-024-00415-2

Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Cranor, L. F., & Koenig, V. (2021). A systematic literature review of empirical methods and risk representation in usable privacy and security research. *ACM Transactions on Computer-Human Interaction*, *28*(6), 1–50. https://doi.org/10.1145/3469845

Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies*, *70*(6), 415–431. https://doi.org/10.1016/j.ijhcs.2012.02.008

F.I. Services. *Global payments report | FIS*. https://www.fisglobal.com/-/media/fisglobal/files/campaigns/global-paymentsreport/FIS_TheGlobalPaymentsReport_2023.pdf

Fagan, M., & Khan, M. M. H. (2016). *Why do they do what they do?: A study of what motivates users to (not) follow computer security advice* [Paper presentation]. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) (pp. 59–75).

Fahl, S., Harbach, M., Acar, Y., & Smith, M. (2013). *On the ecological validity of a password study* [Paper presentation]. Proceedings of the ninth symposium on usable privacy and security (p. 13). ACM. https://doi.org/10.1145/2501604.2501617

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80–92. https://doi.org/10.1177/160940690600500107

Florêncio, D., Herley, C., & Van Oorschot, P. C. (2014). *Password portfolios and the {Finite-Effort} User: Sustainably managing large numbers of accounts* [Paper presentation]. 23rd USENIX Security Symposium (USENIX Security 14) (pp. 575–590).

Frik, A., & Gaudeul, A. (2020). A measure of the implicit value of privacy under risk. *Journal of Consumer Marketing*, *37*(4), 457–472. https://doi.org/10.1108/JCM-06-2019-3286

Frimpong, J. A., & Helleringer, S. (2021). Strategies to increase downloads of covid–19 exposure notification apps: A discrete choice experiment. *PloS One*, *16*(11), e0258945. https://doi.org/10.1371/journal.pone.0258945

Ghose, A., Smith, M. D., & Telang, R. (2006). Internet exchanges for used books: An empirical analysis of product cannibalization and welfare impact. *Information Systems Research*, *17*(1), 3–19. https://doi.org/10.1287/isre.1050.0072

Google (2023). *Google security infographic*. https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Greenstein, S., & McDevitt, R. C. (2011). The broadband bonus: Estimating broadband internet's economic value. *Telecommunications Policy*, *35*(7), 617–632. https://doi.org/10.1016/j.telpol.2011.05.001

Hainmueller, J., Hopkins, D. J., & Yamamoto, T. (2014). Causal inference in conjoint analysis: Understanding multidimensional choices via stated preference experiments. *Political Analysis*, *22*(1), 1–30. https://doi.org/10.1093/pan/mpt024

Hammann, S., Crabb, M., Radomirovic, S., Sasse, R., & Basin, D. (2022). *I'm surprised so much is connected* [Paper presentation]. Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (pp. 1–13). https://doi.org/10.1145/3491102.3502125

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13–42. https://doi.org/10.2753/MIS0742-1222240202

Hassidim, A., Marciano, D., Romm, A., & Shorrer, R. I. (2017). The mechanism is truthful, why aren't you? *American Economic Review*, *107*(5), 220–224. https://doi.org/10.1257/aer.p20171027

Herley, C. (2009). *So long, and no thanks for the externalities: The rational rejection of security advice by users* [Paper presentation]. Proceedings of the 2009 Workshop on New Security Paradigms Workshop (pp. 133–144). ACM. https://doi.org/10.1145/1719030.171905

Herzog, B. (2018). Valuation of digital platforms: Experimental evidence for google and facebook. *International Journal of Financial Studies*, *6*(4), 87. https://doi.org/10.3390/ijfs6040087

Hirschprung, R., Toch, E., Bolton, F., & Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, *61*, 443–453. https://doi.org/10.1016/j.chb.2016.03.033

Huang, D. L., Rau, P. L. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on it adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870–883. https://doi.org/10.1016/j.ijhcs.2011.07.007

Huberman, B. A., Adar, E., & Fine, L. R. (2005). Valuating privacy. *IEEE Security and Privacy Magazine*, *3*(5), 22–25. https://doi.org/10.1109/MSP.2005.137

Hurwicz, L. (1972). On informationally decentralized systems. *Decision and organization: A volume in Honor of J. Marschak*.

Ibrahim, T., Furnell, S. M., Papadaki, M., & Clarke, N. L. (2010). *Assessing the usability of end-user security software* [Paper presentation]. Trust, Privacy and Security in Digital Business: 7th International Conference, TrustBus 2010, Bilbao, Spain, August 30-31, 2010. Proceedings 7 (pp. 177–189). Springer. https://doi.org/10.1007/978-3-642-15152-1_16

Kautondokwa, P., Ruhwanya, Z., & Ophoff, J. (2021). *Environmental uncertainty and end-user security behaviour: A study during the COVID-19 pandemic* [Paper presentation]. IFIP World Conference on Information Security Education (pp. 111–125). Springer. https://doi.org/10.1007/978-3-030-80865-5_8

Khan, M. T., Tran, C., Singh, S., Vasilkov, D., Kanich, C., Ur, B., & Zheleva, E. (2021). *Helping users automatically find and manage sensitive, expendable files in cloud storage* [Paper presentation]. 30th USENIX Security Symposium (USENIX Security 21), USENIX Association (pp. 1145–1162). https://www.usenix.org/conference/usenixsecurity21/presentation/khan-mohammad

Krueger, R. A. (2014). *Focus groups: A practical guide for applied research*. Sage publications.

Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: A survey of westin's studies*.

Li, X. B., Liu, X., & Motiwalla, L. (2021). Valuing personal data with privacy consideration. *Decision Sciences: journal of Innovative Education*, *52*(2), 393–426. https://doi.org/10.1111/deci.12442

Liu, Y., Jia, Y., Tan, Q., Liu, Z., & Xing, L. (2022). *How are your zombie accounts? Understanding users' practices and expectations on mobile app account deletion* [Paper presentation].31st USENIX security symposium (USENIX Security 22) (pp. 863–880).

Lucking-Reiley, D. (2000). Vickrey auctions in practice: From nineteenth-century philately to twenty-first-century e-commerce. *Journal of Economic Perspectives*, *14*(3), 183–192. https://doi.org/10.1257/jep.14.3.183

McClain, C., Faverio, M., Anderson, M., Park, E. (2023). *How Americans view data privacy*. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

Molin, E., Meeuwisse, K., Pieters, W., & Chorus, C. (2018). Secure or usable computers? revealing employees' perceptions and trade-offs by means of a discrete choice experiment. *Computers & Security*, *77*(C), 65–78. https://doi.org/10.1016/j.cose.2018.03.003

Morrison, B., Coventry, L., & Briggs, P. (2021). How do older adults feel about engaging with cyber-security? *Human Behavior and Emerging Technologies*, *3*(5), 1033–1049. https://doi.org/10.1002/hbe2.291

Mosquera, R., Odunowo, M., McNamara, T., Guo, X., & Petrie, R. (2020). The economic effects of facebook. *Experimental Economics*, *23*(2), 575–602. https://doi.org/10.1007/s10683-019-09625-y

Munyendo, C. W., Acar, Y., & Aviv, A. J. (2023). *"In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya* [Paper presentation]. 2023 IEEE Symposium on Security and Privacy (SP), IEEE (pp. 570–587). https://doi.org/10.1109/SP46215.2023.10179410

Murray, H., & Malone, D. (2023). Costs and benefits of authentication advice. *ACM Transactions on Privacy and Security*, *26*(3), 1–35. https://doi.org/10.1145/3588031

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev*, *79*(1), 119.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

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

Pacheco, E. (2024). *Older adults' safety and security online: A post-pandemic exploration of attitudes and behaviors*. arXiv preprint arXiv:240309208.

Page, X., Berrios, S., Wilkinson, D., & Wisniewski, P. J. (2022). Social media and privacy. In *Modern socio-technical perspectives on privacy* (pp. 113–147). Springer International Publishing.

Peddinti, S. T., Korolova, A., Bursztein, E., & Sampemane, G. (2014). *Cloak and swagger: Under- standing data sensitivity through the lens of user anonymity* [Paper presentation]. 2014 IEEE symposium on security and privacy, IEEE (pp. 493–508).

Petrykina, Y., Schwartz-Chassidim, H., & Toch, E. (2021). Nudging users towards online safety using gamified environments. *Computers & Security*, *108*, 102270. https://doi.org/10.1016/j.cose.2021.102270

Prince, J. T., & Wallsten, S. (2022). How much is privacy worth around the world and across platforms? *Journal of Economics & Management Strategy*, *31*(4), 841–861. https://doi.org/10.1111/jems.12481

Qualtrics (2020). *Qualtrics*, https://www.qualtrics.com

Redmiles, E. M. (2019). *Should I Worry?" A cross-cultural examination of account security incident response* [Paper presentation]. 2019 IEEE Symposium on Security and Privacy (SP). IEEE (pp. 920–934). https://doi.org/10.1109/SP.2019.00059

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2019). How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples. *IEEE Security & Privacy*, 1326–1343. https://doi.org/10.1109/SP.2019.00014

Redmiles, E. M., Mazurek, M. L., & Dickerson, J. P. (2018). *Dancing pigs or externalities?: Measuring the rationality of security decisions* [Paper presentation]. Proceedings of the 2018 ACM Conference on Economics and Computation. ACM (pp. 215–232). https://dl.acm.org/doi/10.1145/3219166.3219185

Rosenthal, R., Rosnow, R., & Kazdin, A. (2009). *Artifacts in behavioral research: Robert Rosenthal and Ralph L. Rosnow's Classic Books*. Oxford University Press.

Sandholm, T. (2000). Issues in computational vickrey auctions. *International Journal of Electronic Commerce*, *4*(3), 107–129. https://doi.org/10.1080/10864415.2000.11518374

Schaub, F., Könings, B., & Weber, M. (2015). Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing*, *14*(1), 34–43. https://doi.org/10.1109/MPRV.2015.5

Scholefield, S., & Shepherd, L. A. (2019). *Gamification techniques for raising cyber security awareness* [Paper presentation]. International conference on human-computer interaction (pp. 191–203). Springer. https://doi.org/10.1007/978-3-030-22351-9_13

Simko, L., Lerner, A., Ibtasam, S., Roesner, F., & Kohno, T. (2018). *Computer security and privacy for refugees in the United States* [Paper presentation]. 2018 IEEE Symposium on Security and Privacy (SP), IEEE (pp. 409–423). https://doi.org/10.1109/SP.2018.00023

Solove, D. J. (2021). The myth of the privacy paradox. *SSRN Electronic Journal*, *89*, 1. https://doi.org/10.2139/ssrn.3536265

Spiekermann, S., & Korunovska, J. (2017). Towards a value theory for personal data. *Journal of Information Technology*, *32*(1), 62–84. https://doi.org/10.1057/jit.2016.4

Spiekermann, S., Korunovska, J., & Bauer, C. (2012). Psychology of ownership and asset defense: Why people value their personal information beyond privacy. *SSRN Electronic Journal*, *32*(1). https://doi.org/10.1057/jit.2016.4

Sun, S., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2011). *What makes users refuse web single sign-on?: An empirical investigation of OpenID* [Paper presentation]. SOUPS '11: Proceedings of the Seventh Symposium on Usable Privacy and Security (pp. 1–20). https://doi.org/10.1145/2078827.2078833

Sweeten, G., Sillence, E., & Neave, N. (2018). Digital hoarding behaviours: Underlying motivations and potential negative consequences. *Computers in Human Behavior*, *85*, 54–60. https://doi.org/10.1016/j.chb.2018.03.031

Takano, Y., Ohta, S., Takahashi, T., Ando, R., & Inoue, T. (2014). *MindYourPrivacy: Design and implementation of a visualization system for third-party Web tracking* [Paper presentation]. 2014 twelfth annual international conference on privacy, security and trust., IEEE (pp. 48–56). https://doi.org/10.1109/PST.2014.6890923

Tan, J., Sharif, M., Bhagavatula, S., Beckerle, M., Mazurek, M. L., & Bauer, L. (2018). *Comparing hypothetical and realistic privacy valuations* [Paper presentation]. Proceedings of the 2018 workshop on privacy in the electronic society (pp. 168–182). https://doi.org/10.1145/3267323.3268961

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness.*, Penguin.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260

Uğur, N. G., & Alışkan, K. C. (2022). Time for de-cluttering: Digital clutter scaling for individuals and enterprises. *Computers & Security*, *119*(C), 102751. https://doi.org/10.1016/j.cose.2022.102751

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., & Cranor, L. F. (2015). *I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab* [Paper presentation]. Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (pp. 123–140).

Vickrey, W. (1961). Counterspeculation, auctions, and competitive sealed tenders. *The Journal of Finance*, *16*(1), 8–37. https://doi.org/10.1111/j.1540-6261.1961.tb02789.x

Wang, R., Chen, S., & Wang, X. (2012). *Signing Me onto Your Accounts through Facebook and Google: A traffic-guided security study of commercially deployed single-sign-on web services* [Paper presentation]. 2012 IEEE symposium on security and privacy (pp. 365–379). https://doi.org/10.1109/SP.2012.30

Wei, M., Mink, J., Eiger, Y., Kohno, T., Redmiles, E. M., & Roesner, F. (2024). *{SoK}(or {SoLK?)}: On the quantitative study of sociodemographic factors and computer security behaviors* [Paper presentation]. 33rd USENIX Security Symposium (USENIX Security 24) (pp. 7011–7030).

About the authors

Shubham Singh is a Postdoctoral Scholar at the University of Chicago Data Science Institute. His research sits at the intersection of algorithmic fairness, security and privacy, and computational social science, with a focus on diagnosing and mitigating biases in sociotechnical systems.

Jackie Hu is a PhD student at the University of Michigan - Ann Arbor, School of Information, researching race, labor, and science and tech policy.

Cormac Herley is at Microsoft Research. He received the BE (Elect) from the National University of Ireland (Cork), the MSEE from Georgia Tech, and the PhD from Columbia University. He has published in the areas of Signal Processing, Information Theory, Multimedia, Computer Security, and Machine Learning.

Elissa M. Redmiles is the Clare Boothe Luce Assistant Professor of Computer Science at Georgetown University and a faculty associate at Harvard University's Berkman Klein Center for Internet & Society. Her award-winning research studies security, privacy, and online safety threats, decision-making, and communication with a focus on addressing inequities.

Siddharth Suri is a computational social scientist at Microsoft Research, analyzing the effects of AI on society.

Oshrat Ayalon is a Senior Lecturer at the University of Haifa and Head of the SoTI Lab (Society and Technology Interaction Lab). Her lab investigates the intersection of human–computer interaction, privacy, security, and online safety, with a focus on minority groups and adolescents.