IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 16, 2022, accepted March 30, 2022, date of publication April 13, 2022, date of current version April 20, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3167025

Degrees of Perceived Control Over Personal Information: Effects of Information Relevance and Levels of Processing

YEFIM SHULMAN AND JOACHIM MEYER, (Senior Member, IEEE)
Department of Industrial Engineering, Tel Aviv University, Tel Aviv 6139001, Israel

Corresponding author: Yefim Shulman (efimshulman@mail.tau.ac.il)

This work was supported in part by the European Union (EU) Horizon 2020 Research and Innovation Program through the Marie Skłodowska-Curie Grant 675730 ''Privacy and Us.''

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Ethics Committee of Tel-Aviv University.

ABSTRACT Major legal, philosophical, and scientific discussions regard control over personal information as a cornerstone of users' fundamental right to privacy. Even though user perceptions of control determine whether and how people exercise their control, little is known about how these perceptions develop. We identify a property of the personal information the online service providers process, naming it the ''Order of Control''. In an online experiment ($N = 329$) with a pre-study ($N = 110$), we investigate how this property and personal information relevance affect users' perceived control across three contexts of disclosure through mobile devices: meet ups, mobile payments, and food delivery. We find that perceived control differs depending on a person's assumptions regarding the required levels of information processing. This effect was moderated by information relevance, albeit not systematically, and differed across the three contexts. The results also reveal that users tend to assume that any personal information may be recoverable from any other disclosed personal data, limiting their control over such information. Privacy practitioners and system designers should consider informing the users regarding outcomes of their disclosure and sharing decisions, while researchers should further investigate how user perceptions of control form and manifest themselves.

INDEX TERMS HCI, perceptions of control, personal information disclosure, personal information processing, privacy, technology social factors.

I. INTRODUCTION

''People desire privacy and more control over their information,'' is a declaration found in the California Consumer Privacy Act of 2018 (CCPA, Section 2, Paragraph (h) [1]). The CCPA followed the enactment of the European Union Data Protection Regulation (GDPR), which itself links data protection with an individual's ability to control their personal data (GDPR Recitals 7, 60-63, 65, 66, 68-70, 75, 85 [2]), specifically stating that, ''Natural persons should have control of their own personal data'' (GDPR Recital 7 [2]). Extraterritorial application of the GDPR[1] conforms the laws worldwide to enable people's control over their personal information (e.g., the United Kingdom Data Protection Act 2018 (c 12), or extending the GDPR's validity to Iceland, Norway, and Lichtenstein). The legislative initiatives are in line with major developments in privacy research, such as Altman's [3] and Westin's [4] definitions of privacy, social contract, social exchange, and reactance theories applied to privacy and consumer behavior [5]–[7], privacy protection goals [8], the APCO model [9], which all converge on the crucial role of control. Empirical research also demonstrates the benefits from empowering people by giving them control over their personal information [10], [11].

Control over personal information has been qualitatively defined as people's right and ability to decide which information about them should be available to others and when the information should be deleted. However, we argue that

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Asif.

[1]American Bar Association, April 2018, url: www.americanbar.org/groups/ business_law/ publications/ blt/ 2018/04/01_speirs

disclosing or deleting personal information do not amount to efficient control. Drawing on the premises of control theory, we emphasize that to effectively control their personal information, users of ubiquitous and complex online systems would not only need to know which information has been disclosed, stored, and processed, but also, crucially, what the consequences of their disclosure or deletion actions have been. When such knowledge is hardly attainable, the users would have to rely on their subjective perceptions of control. In fact, such perceptions were shown to impact user decision-making regarding disclosure [12]–[14]. Despite jurisprudence and empirical privacy research agreeing on the importance of personal information control and tangible effects of its perception, little is known about how users form their perceptions of control over the personal information they make available to the service providers.

We report here a two-phase study, in which we investigate users' perceptions of control based on the assumptions and beliefs the users may have regarding the service providers' data processing abilities. We conjecture that such perceptions should measurably reflect the level of effort to control data, based on the perceived intensity of the service providers' processing practices. To accommodate this conjecture, we draw on the concept of the ''Order of Control'' (OOC, inspired by the homonymous term from control theory) as a property of processed data, supposed to be controlled. Assuming that the OOC increases with the amount of processing, we hypothesize that perceived user control will decrease. We test whether and to what extent such a single property can help formalize and explain user perceptions of control. To address the potential contextual dependence of such assumptions, we vary the relevance of personal information items (PIIs), and put them in three contexts, namely, three different types of mobile applications: meet up, mobile wallet, and food delivery. We selected the three contexts to represent relatively common activities, in which users regularly engage: social, financial, and utility interactions, respectively. We measure the perceptions of control as the extent to which users believe that one PII can be learned from one or more PIIs. The results show that the *perceived control* over PIIs indeed decreases following the increase in the OOC, providing support for the OOC as a useful concept for studying user control over personal information. The relation between perceptions and assumptions is shown to depend upon the relevance of the PII for a given context. Interestingly, our findings demonstrate that users tend to assume that any personal information can be reasonably learned from any other personal information, indicating that it may be only a matter of effort, which would differ based on the amount of processing.

II. BACKGROUND

A. PERCEIVED CONTROL OVER PERSONAL INFORMATION

The individual's ability to give or revoke consent to the processing of their personal information is essential for the paradigms, in which privacy is defined as control over personal information [3], [4], [15]–[17]. Users of online systems and services exercise their control by deciding to disclose and share their personal information, as well as consenting to policies through the ''informed consent'' mechanism. Such decisions are naturally informed by the users' experiences and knowledge, the reputation of the service provider, contextual and momentary factors, etc. The users' perceptions of control develop and form out of the combination of such factors.

The concept of perceived control or control perceptions is profoundly present in the privacy literature [18]. Perceived control has usually been operationalized among the antecedents of privacy behavior [9], affecting or interacting with privacy concerns [19], [20], risk perceptions [21], [22], trust [19], willingness to disclose information and disclosure behavior [23], [24], affective states [24], and other constructs. Perceived control may result in risk-compensation behavior among users who disclose information on online social networks [13], [25], or by interacting with privacy policies, notifications, and webforms [26]–[28]. In its turn, perceived control may be influenced by feedback on how personal information has been used or how others may have disclosed it [29]. Opt-in privacy policies may tend to increase perceived control, compared with opt-out policies [30]. Crucially, perceived control over personal information may be dramatically affected by mere design changes (i.e., external information users may receive from online systems), even though actual control remained perfectly unaltered [31]. Thus, perceived control informs users' disclosure and sharing decisions, which can be interpreted as control actions vis-à-vis their personal information.

B. PARAMETERIZING CONTROL OVER PERSONAL INFORMATION

1) ORDER OF CONTROL

We draw upon the framework of control theory [32], [33], which formally investigates control over complex systems and processes. A typical control system consists of a controller, a control actuator, a controlled plant, and an optional feedback loop. In the case of personal information control, we suggest the conceptual model shown in Fig. 1. A controller is a *person* — a *user* of an online system or service. An actuator is any tool or mechanism the user may use to disclose, modify, or remove their personal information (*controls*). A controlled plant is some *process* involving personal information disclosure and sharing, which the user tries to control (e.g., using an online marketplace, social network, mobile wallet application). Such a process or the process holder (i.e., data controller or data processor in terms of the GDPR) may request personal information belonging to the user. As a result, some personal information — *[personal information]'* — becomes available to the process or the process holder. A *feedback* mechanism is necessary to inform users about the outcomes of their control actions, including but not limited to the categories of personal information being revealed and ways this information is being processed. The perceptions of control are characteristics of the user.

In control theory, the order of the control system is the highest order of a particular differential equation defining the behavior of the controlled plant [34]. Borrowing this term, we conceptualize the *Order of Control* (OOC) as a general property of the information [35]. Defining it more narrowly, in this paper, the OOC sets the user's assumptions (perhaps learned through feedback [29]) regarding the use of their personal information, being held and processed by a service provider. This way the OOC corresponds to the phenomena, whereby the perceived control over personal information changes in response to the user interface design without any changes in the actual level of control [31], as well as to situations, where changes in perceived control can be explained by changes in the actual control (e.g., [30], [36]). Table 1 illustrates our conceptualization of the OOC. The example of the OOC for personal information control relates to processing over time or the required amount of data processing (as the perceived amount of data processing has been shown to affect customers' trust and perceived risk [37]). Another example may show the OOC as a function of the amount of collected data (from one fact to multiple facts, to information collected over time, to combining information from third parties, etc.). For the purpose of this paper, we opertionalize a combination of both examples in Section IV.

If the OOC as a single property can reflect and influence user perceptions of control (through the feedback the user receives while interacting with the process, Fig. 1), it may provide an insight into decision-making regarding personal information disclosure, and establish a baseline for the study of user control over personal information. However, the OOC does not act upon user perceptions in isolation. In this paper, we also address the relevance of personal information being disclosed or controlled, which may profoundly affect user perceptions of control.

2) INFORMATION RELEVANCE

User perceptions of control develop as a result of a complex process, involving experience, prior knowledge, mental models, emotional states, a service provider's reputation, etc. One crucial factor in this process is personal information relevance, which is especially prominent for our investigation. Our model (Fig. 1) implies that people form their control perceptions, based on the PIIs they are requested to disclose (i.e., the personal information requests), the context of the disclosure, and the external information and knowledge available to them at the time of disclosure.

The relevance of the personal information a service provider requests has been shown to influence privacy risk perceptions and attitudes to information disclosure [39], [40]. Crucially, the effect of information relevance on the latter may be highly context-dependent [41]. In online advertising, information relevance (or ''utility'') appears to be positively associated with purchase intentions [42], customer self-awareness [43], and attitudes towards the advertisement or brand holder [44], while mitigating concerns regarding privacy invasion [43]. Thus, information relevance can affect users' attitudes, both when the users are required to disclose it (e.g., a social network asking users for their names), and when the service providers try to engage customers into an interaction (e.g., marketing notifications, ads). In this paper, we rely on people's judgments to gain ad hoc estimates of relevance. We explore whether and how personal information relevance may alter the relation between the OOC and perceptions of control (Fig. 1).

Therefore, to empirically explore the concept of the *Order of Control* in control over personal information, we inquire,
RQ: How does the Order of Control (i.e., control afforded at different distinctive levels) affect people's perceptions of control over their personal information? We predict: noitemsep

P1: An inverse relation exists between the Order of Control (as conceptualized in Section II-B1) and perceived control over personal information: with an increase in the Order of Control, perceived control decreases.

P2: The relation between the Order of Control and perceived control over personal information depends on the relevance of a personal information item for the situation.

III. PRELIMINARY STUDY: INFORMATION RELEVANCE ESTIMATES IN DIFFERENT CONTEXTS

We conducted an online study to learn people's estimates of the relevance of various personal information items (PIIs, e.g., name, current location) for three different contexts. The *Relevance* judgements we obtained in this preliminary study serve us in the subsequent experiment (Section IV).

A. DESIGN, MATERIALS, AND PROCEDURE

We selected three common types of apps to represent the three *Contexts*: (1) a *Meet up* application as an example of a peer-to-peer interaction facilitating social behavior; (2) a *Mobile wallet* application as an example of an app eliciting financial considerations; (3) a *Food delivery* app as an example of a utility service, facilitating attitudes related to convenience and shopping.

We asked the participants in the preliminary study to judge the relevance of 34 PIIs for the three apps. Given the exploratory nature of the study and intending not to over-burden the participants' attentiveness, we did not aim for the list of the PIIs to be exhaustive. However, to make it as comprehensive as possible, we developed the list of the PIIs, considering the special categories of personal data under the GDPR and typical permissions requested by apps on Android and iOS. The participants indicated the relevance of each item on a 4-point Likert-type scale, anchored ''Irrelevant'' through ''Relevant''.[2] The list of the PIIs and detailed instructions can be found in Appendix A. The study was implemented with the Qualtrics platform[3] and was accessible via a link on the participants' desktop and mobile devices.

[2]Both in the preliminary study and the ensuing experiment, we controlled common method variance through available procedural remedies in the design of the studies: separation of measurement, accentuating participants' anonymity, reducing evaluation apprehension, etc. [45].

[3]Qualtrics LLC, Provo, Utah, US.

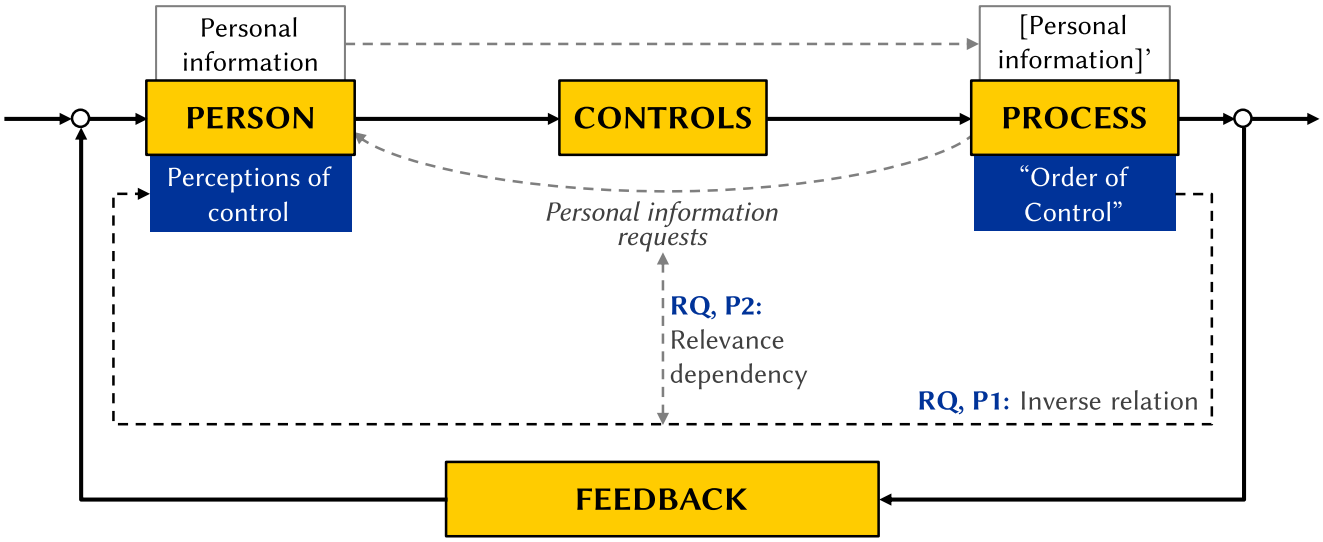


FIGURE 1. Conceptual control model: control over personal information (adapted from [38]).

TABLE 1. Order of Control in control over personal information.

Order of Control	Manual control	Control over personal information	Example
0	Position	A meaningful and complete PII (i.e., a fact)	Medical diagnosis, treatment; sexual orientation, etc.
1	Speed	Pieces of the PII, accumulation of which over time may allow to piece together the PII	Calendar events, meetings, appointments, knowledge of which over time may allow to learn about the diagnosis, sexual orientation, etc.
2	Acceleration	Data, aggregation of which over time may allow to infer the pieces, accumulation of which over time may allow to piece together the PII	Location tracking, timestamps, residential and business addresses, knowledge of which over time may allow to infer the information about the meetings, appointments, etc.
3 and higher	Jerk, jounce, "crackle and pop", etc.	Higher granularity data or metadata → data of Order 2 → pieces of Order 1 → the PII	(Meta)data provided by the network carrier's base stations, allowing to recover locations over time, allowing to infer the meetings, appointments, and so on...

B. PARTICIPANTS

We used the CloudResearch platform to recruit English speaking residents of the USA for the study. We collected 117 full responses. Upon closer inspection, seven participants were excluded for answering in repetitive patterns, leaving us with $N = 110$ participants. Most participants reported their gender as female ($n = 64$, 58.2%), with the rest reporting male ($n = 46$, 41.8%). Most participants reported "Bachelors's degree or an equivalent" as their highest completed level of education ($n = 37$, 33.6%). The largest age cohort was "60–64" ($n = 22$, 20.0%). Appendix A-C contains the detailed sample demographics.

Participation in the study was voluntary, with remuneration provided upon its completion.[4] The participants were able to terminate their involvement in our research at any point, with no negative consequences for themselves. They were instructed accordingly, and had to acknowledge the consent form before taking part in the study. The university's ethical committee approved the study and the informed consent form.

C. RESULTS

The PII *Relevance* ratings did not differ significantly across participants as a function of an age cohort (we aggregated the age cohorts into three groups of comparatively equal size). The type of answer to the attentiveness check question (numerical vs. verbal response) also did not affect responses significantly. Therefore, we obtained sets of items for the three categories of *Relevance* for each app: *Irrelevant*, *Neutral* (i.e., neither relevant nor irrelevant), and *Relevant* items.[5]

[4] As per CloudResearch, "Upon completion of the study, you will receive compensation in the amount that you have agreed to with the platform through which you entered this survey."

[5] Reliability measures were Cronbach's $\alpha = 0.94$ for *Meet up*, $\alpha = 0.92$ for *Mobile wallet*, and $\alpha = 0.90$ for *Food delivery*.

Assignment to the categories was done based on the mean *Relevance* ratings. From these sets we selected a single item per *Relevance* category per app based on the *Relevance* statistics (Table 2).

IV. EXPERIMENT: ORDER OF CONTROL OVER PERSONAL INFORMATION

We used the results of the preliminary study (Section III) in the design of the online experiment to learn how people perceive control over their personal information and whether such perceptions can reflect and be set by discrete levels of control, i.e., the OOC.

A. DESIGN

1) INDEPENDENT VARIABLES

We included the three *Contexts* from the preliminary study (Section III), represented by *Meet up*, *Mobile wallet*, and *Food delivery* applications, to be able to improve the generalizability of the results. For each app, we selected three PIIs, differing in the level of *Relevance* (Table 2): *Irrelevant*, *Neutral*, and *Relevant*. We term these PIIs *disclosed* (DPII) because, in the context of the experiment, the disclosure of any of these PIIs to the service provider (i.e., app owner) might allow learning of other PIIs — *learnable* PIIs (LPII) — by the service provider to some reasonable degree.

We selected five LPIIs for each DPII from the same list developed in the preliminary study (Section III, Appendix A-A). The LPIIs were drawn to fit each app type under the assumption that the amount of processing needed to obtain an LPII increases for the five LPIIs, while direct user control over them decreases. These changes in user control and the amount of required processing represent the *Order of Control*. We assumed that four of the LPIIs could be reasonably inferred from collecting the DPII over time and (or) juxtaposing this DPII with other data the service provider would have. Learning of the fifth LPII for each DPII from any data available to the service provider was, in contrast, intended to appear as least reasonable for any individual.

Thus, the study had a $3 \times [3 \times 5]$ mixed complete factorial design: three different *Contexts* (apps, between-subjects) by three levels of the DPII *Relevance* (*Irrelevant–Neutral–Relevant*, within-subjects) by five levels of the *Order of Control* (0 through 4, within-subjects). Table 3 contains the breakdown of the independent variables: the LPIIs per DPII per *Context*.

2) DEPENDENT VARIABLE

We asked the participants to estimate the possibility of a PII to be *learned* (i.e., discovered by the entity, who owns a given app) from each DPII: ''If you give this information, how possible is it for the company who owns the application to learn…'' To provide their estimations, the participants used a 10-point semantic differential scale, anchored ''Not possible at all'' – ''Easily possible'' for each LPII. This measure of the *Perceived Effort to Learn Personal Information* (PELPI) constituted the dependent variable in the study.

3) COVARIATE

We also measured participants' *Perceived Information Control* (PIC) as a general attitude towards their respective type of app, using a scale adapted from Dinev *et al.* [22]. The scale contains 4 items, measuring PIC on a 7-point Likert scale, anchored ''Strongly disagree'' through ''Strongly agree''. The details of the used scale and the instructions shown to the participants are provided in Appendix B-A.

The study was implemented using the Qualtrics platform and was accessible via a link on the participants' own desktop and mobile devices.

B. PROCEDURE

The study included four consecutive stages: enrollment, main stage, questionnaires, and disenrollment.

1) ENROLLMENT

The participants followed the link to access the study with their own devices. First, we asked them to acknowledge the informed consent form. Next, as a precaution against automated responses, we asked the participants to pass a reCAPTHCA check and answer an attentiveness question.

2) MAIN STAGE

The participants were shown the instructions for the study. In the instructions, we described the exact type of app (out of the three possible types of apps) the participant should think about when answering the questions that were to follow. Next, the participant estimated the possibility of learning information (LPII) from the disclosure of other information (DPII): 5 items of LPII (corresponding to the levels of the *Order of Control*) per 3 types of DPII (*Relevance*) per app (*Context*), thus answering $5 \times 3 = 15$ questions each. Each DPII was presented separately in a randomized sequence, followed by the five corresponding LPIIs, presented all on the same page in a randomized order.

3) QUESTIONNAIRES

First, the participants responded to the four items measuring their PIC in the context of their respective type of app. The items were shown in a randomized order. Then, we asked the participants whether they had previous experiences with the respective type of app, and whether they had any thoughts or feelings regarding that type of app (Appendix B-C). Next, the participants answered the demographics questions about their age cohort, gender, and the highest completed level of education.

4) DISENROLLMENT

The participants reported whether they were able to pay attention to the task (an honesty-based attention check). Then, they were invited to share with the researchers any thoughts or concerns they might have had regarding the study. Finally, the participants were redirected to the experiment platform to receive instructions on their remuneration.

TABLE 2. Personal information items (PIIs) selected for the experiment.

PII relevance	Meet up app		Mobile wallet app		Food delivery app	
	Item	*M (SD)*	*Item*	*M (SD)*	*Item*	*M (SD)*
Relevant	"Your interests and hobbies"	3.34 (0.85)	"Your bank information"	3.10 (1.02)	"Your current location"	3.45 (0.96)
Neutral	"Your current location"	2.65 (1.12)	"Your purchases"	2.53 (1.12)	"Your dietary preferences"	2.35 (1.19)
Irrelevant	"Your bank information"	1.17 (0.54)	"Your interests and hobbies"	1.26 (0.69)	"Your memberships in organizations [...]"	1.12 (0.44)

Note: All means and standard deviations calculated based on the range of values: $1-4$.

TABLE 3. Learned Personal Information Items by Disclosed Personal Information Items by the Order of Control (OOC).

OOC	Relevance of Disclosed Personal Information Items		
	Relevant	*Neutral*	*Irrelevant*
	Meet up app		
	"Your interests and hobbies"	*"Your location"*	*"Your bank information"*
0	"your bank account number"	"your current location"	"your preferences for pastime"
1	"where you live"	"where you live"	"places you visit(ed)"
2	"purchases you make"	"the names of your friends and relatives"	"your health and physical shape"
3	"your tax paying history"	"your medical conditions and treatments"	"your memberships in organizations"
4	"your genetic predispositions to diseases"	"your fingerprint patterns"	"your credit history"
	Mobile wallet app		
	"Your bank information"	*"Purchases you make"*	*"Your interests and hobbies"*
0	"your bank account number"	"your food preferences"	"your preferences for pastime"
1	"where you live"	"where you live"	"places you visit(ed)"
2	"your employment history"	"details of your salary and incomes"	"your memberships in organizations"
3	"your tax paying history"	"the details of your education"	"your credit history"
4	"your genetic predispositions to diseases"	"your citizenship(s)"	"your physiological state (lung capacity, heart rate)"
	Food delivery app		
	"Your location"	*"Your dietary preferences and restrictions"*	*"Your memberships in organizations"*
0	"your current location"	"your preferred foods"	"the affiliations with" such organiztions"
1	"where you live"	"your health conditions and treatments"	"where you live"
2	"the names of your friends and relatives"	"where you work"	"your political leanings and religious beliefs"
3	"your medical conditions and treatments"	"details of your salary and incomes"	"details of your salary and incomes"
4	"your fingerprint patterns"	"details of your criminal records"	"recordings of your voice"

Note: the Order of Control levels:
0: Learned immediately;
1: Learned over time;
2: Learned over time after juxtaposing with other data available to the service provider;
3: Learned over time after juxtaposing with third party databases;
4: Learning could appear unreasonable (unrelated).

C. PARTICIPANTS

Here, too, we used the CloudResearch platform to recruit English speaking USA residents as participants. Having estimated the minimal required sample size using G*Power 3 [46], overall, we collected $N = 329$ valid responses. Most participants ($n = 219$, 66.6%) completed the study using mobile platforms, while the rest ($n = 110$, 33.4%) used a desktop or laptop platforms. The majority

of participants reported their gender as female ($n = 204$, 62.0%), $n = 2$ (0.6%) participants identified as "Other / None of the above / Non-binary" with the rest being male ($n = 123$, 37.4%). Most participants reported "Bachelors's degree or an equivalent" as their highest completed level of education ($n = 87$, 26.4%), followed by $n = 67$ (20.4%) having received "High school diploma or an equivalent", $n = 60$ (18.2%) — "Some college credit, no degree", $n = 41$ (12.5%) — "Associate's degree or an equivalent", $n = 39$ (11.9%) — "Master's degree or an equivalent", $n = 14$ (4.3%) — "Doctorate degree or an equivalent", $n = 10$ (3.0%) for each "Trade, technical, vocational training" and "Some high school, no diploma", and $n = 1$ (0.3%) preferred not to disclose this information. The largest age cohort was "35–39" ($n = 59$, 17.9%), followed by "25–29" ($n = 52$, 15.8%), "30–34" ($n = 47$, 14.3%), "40–44" ($n = 34$, 10.3%), "18–24" ($n = 33$, 10.0%), "50–54" ($n = 24$, 7.3%), "45–49" and "65–69" (both $n = 19$, 5.8%), "55–59" ($n = 15$, 4.6%), "70–74" ($n = 11$, 3.4%), "60–64" ($n = 10$, 3.0%), "75–79" ($n = 4$, 1.2%), and "80–84" ($n = 2$, 0.6%).

A large number of participants ($n = 139$, 42.3%) reported use of the apps from their respective context, while the majority ($n = 164$, 49.8%) reported not to be active users. Twenty two participants (6.7%) opted for "I don't know", while $n = 4$ (1.2%) refused to answer. The distribution of participants across contexts was comparable: 34, 56, and 49 among the active users; and 68, 45, and 51 among non active users for *Meet up*, *Mobile wallet*, and *Food delivery*, respectively.

Participation in the study was voluntary, and the participants were remunerated upon its completion in accordance with CloudResearch panels' rates. The participants were able to terminate their involvement in our research at any point, with no negative consequences for themselves. They were instructed accordingly, and had to acknowledge the consent form before taking part in the study. The study and the informed consent form underwent the university's ethical committee approval process.

V. EXPERIMENT RESULTS

A. PREPARATORY ANALYSIS

In the experiment, we used the *Perceived Information Control* scale (PIC) to measure the participants' general perceptions of control over personal information towards a respective app type (*Meet up*, *Mobile wallet*, or *Food delivery*).

To ensure the reliability of the results, we checked the correctness of the measurement of PIC, running a principal component analysis (PCA). The PCA with orthogonal rotation showed that all 4 items loaded into a single factor, as expected, explaining 81.56% of the cumulative variance in the items. Sampling adequacy was acceptable according to a Kaiser-Meyer-Olking (KMO) overall measure of 0.84 [47] (all anti-image correlations being 0.84 or higher, participant-to-item ratio of 82.25 : 1). Bartlett's test of sphericity was significant at $p < 0.001$, indicating that the items were suitable for an exploratory factor analysis. The reliability of the measurement was also acceptable, estimated with a Cronbach's $\alpha = 0.92$ (higher than the recommended level of 0.70 [48]). Removal of any of the four items did not increase the level of reliability. Therefore, the PIC score was calculated for each participant as an average of all four items.

Overall, the participants reported a level of PIC at $M = 4.53$, $SD = 1.59$, $Mdn = 4.75$, range: $1 - 7$. Those in the *Meet up* condition reported PIC at $M = 4.34$, $SD = 1.55$, $Mdn = 4.50$, range: $1 - 7$, while those in the *Mobile wallet* condition reported PIC at $M = 4.55$, $SD = 1.71$, $Mdn = 4.75$, range: $1 - 7$, and those in the *Food delivery* condition — at $M = 4.72$, $SD = 1.50$, $Mdn = 5.00$, range: $1 - 7$. The PIC measure and the app type did not correlate significantly, and the difference in the means across the app types was not significant.

B. EFFECTS OF RELEVANCE OF DISCLOSED PERSONAL INFORMATION ITEMS AND THE ORDER OF CONTROL ON THE PERCEIVED EFFORT TO LEARN PERSONAL INFORMATION

We tested the effects of our independent variables (DPII *Relevance* and the *Order of Control*) on the *Perceived Effort to Learn Personal Information* (PELPI) in a repeated measures analysis of covariance (ANCOVA), having checked the necessary ANCOVA assumptions.

1) MAIN MODEL

The ANCOVA model included PIC as a covariate. The *Context* (i.e., app types) was intended to improve the generalizability of the results and, therefore, was not included in that ANCOVA model as another independent variable. Appendix B-B contains the full results of an extended ANCOVA model, which included *Context* as a between-subjects factor, while Section V-B2 highlights the extended model's results.

As the model mildly violated the assumption of sphericity (Mauchly's test at p<0.01 for all effects), we report the results based on a Greenhouse-Geisser correction to the degrees of freedom [49]. The data revealed a main effect of the OOC on the PELPI, $F(2.39, 781.29) = 53.48$, $p < 0.001$, $\eta_p^2 = 0.14$. The significant differences were found between the levels of the OOC (in Bonferroni-adjusted 95% confidence intervals (CI) of mean differences, all $p < 0.001$): 0 vs. 2 CI[0.72, 1.40], 0 vs. 3 CI[1.19, 2.00], 0 vs. 4 CI[1.94, 2.86], 1 vs. 2 CI[0.81, 1.40], 1 vs. 3 CI[1.29, 1.98], 1 vs. 4 CI[2.04, 2.84], 2 vs. 3 CI[0.29, 0.77], 2 vs. 4 CI[1.03, 1.64], 3 vs. 4 CI[0.55, 1.06]. The only not significant difference was between the levels 0 and 1. The participants tended to express the PELPI, which decreased significantly with increase in each level of the OOC (apart from OOC 0 and 1): from OOC 0 and 1 ($M = 7.25$, $SE = 0.12$ and $M = 7.29$, $SE = 0.12$, respectively), through OOC 2 ($M = 6.19$, $SE = 0.13$) and OOC 3 ($M = 5.66$, $SE = 0.14$) to OOC 4 ($M = 4.85$, $SE = 0.15$).

We also found a main effect of *Relevance* on the PELPI, $F(1.93, 630.78) = 2.46$, $p = 0.09$, $\eta_p^2 = 0.01$.

The significant differences (Bonferroni-adjusted) were found in *Irrelevant* vs. *Neutral*, $p = 0.034$, mean difference CI[0.01, 0.50], and *Relevant* vs. *Neutral*, $p = 0.028$, mean difference CI[0.02, 0.43] comparisons. The participants tended to express higher PELPI for the *Irrelevant* ($M = 6.34, SE = 0.12$) and *Relevant* ($M = 6.31, SE = 0.12$) DPIIs than for the *Neutral* DPII ($M = 6.09, SE = 0.13$).

Importantly, the data revealed a significant *Relevance* × *OOC* interaction, $F(7.45, 2437.12) = 2.72$, $p < 0.01$, $\eta_p^2 = 0.01$ (Fig. 2). A priori contrasts showed a significant linear decrease of the PELPI with an increase in the OOC, $F = 84.36$, $p < 0.001$, $\eta_p^2 = 0.20$, as well as a significant quadratic (OOC) effect, $F = 20.99$, $p < 0.001$, $\eta_p^2 = 0.06$. The Šidák-corrected multiple comparisons revealed significant differences between the levels of the DPII *Relevance* within some of the levels of the OOC. Within the OOC 0, there were significant differences between the *Irrelevant* DPII and the other two levels of *Relevance*, both at $p < 0.005$, with no difference between the *Neutral* and *Relevant* DPIIs. No significant differences between the levels of *Relevance* were found within the OOC 1. Similarly to the OOC 0, significant differences were found within the OOC 2 between the *Irrelevant* DPII and the other two levels of *Relevance*, both at $p < 0.001$, but no significant difference between the other two levels of *Relevance* themselves. Within the OOC 3, the significant differences were found between the *Neutral* DPII and the other two levels of *Relevance*, both at $p < 0.001$, with no significant difference between the *Irrelevant* and *Relevant* levels of DPII *Relevance*. Finally, no significant differences between the levels of DPII *Relevance* were found within the OOC 4. Overall, the interaction reveals a clear decreasing pattern of the PELPI along the increase in the OOC from OOC 0 and 1 through OOC 4, with unsystematic, yet significant, differences between the levels of *Relevance* of the DPIIs (Fig. 2).

2) MODEL INCLUDING CONTEXT

If we include the *Context* as a between-subjects factor in the model, the overall effect of the three-way *Context* × *OOC* × *Relevance* interaction is larger than the effect of the two-way interaction (excluding *Context*), $F(15.15, 2462.39) = 8.89$, $p < 0.001$, $\eta_p^2 = 0.05$. Other aforementioned effects get stronger, as well (Appendix B-B). The *Context* indeed mattered (Fig. 3). It made the PELPI generally the highest for the *Mobile wallet* app for any DPII *Relevance*. It also made the PELPI decrease faster for the *Food delivery* app for any DPII *Relevance*. The PELPI behaved most similarly across all *Contexts* when the DPII was *Irrelevant*.

VI. DISCUSSION

In this paper, we focused on user perceptions of control over personal information as an important factor that can both facilitate and reflect the actual control over personal information the users may have. We aimed to advance research on how such user control can be understood and more efficiently implemented. Being inspired by control theory, we drew on the concept of the ''Order of Control'', using it verbatim, but conceptualizing it as a property of personal information being processed by the service providers. We investigated how the OOC affected people's perceptions of control over their personal information (RQ), predicting them having an inverse relation (P1), which would depend on the *Relevance* of a personal information item for a particular situation (P2).

A. IMPLICATIONS AND INSIGHT

Our findings reveal the effects of the *Order of Control* and the *Relevance* of personal information items on people's perceived control, offering several meaningful implications for research and practice.

1) ORDER OF CONTROL AND PERCEPTIONS OF CONTROL

Participants revealed their beliefs about the possible uses of their personal information. The *Order of Control* over their disclosed personal information indeed affected these beliefs. Users' perceived control decreased when the level of processing and access to third-party data increased, supporting our first prediction (P1). Thus, users have reasonable perceptions of data processing, based on their experiences and knowledge. The results demonstrated that the proposed approach in general, and the OOC concept in particular, can contribute to the study of control over personal information. As described in Section II-B1, the OOC should also be explored as a function of processing over time or as the amount of already available personal data. The OOC can potentially be used to categorize data processing practices and translate their effects to the users of online systems. The OOC may also be able to help develop a measure of effective control for system evaluation. Additionally, we suggest that the OOC may be used to relate actual with perceived control and build a control taxonomy to inform system design and implementation. Further, more work is needed to establish other crucial elements of the conceptual control model and their effects on personal information control.

Participants indicated that learning new information about them by using the PII with the highest level of the OOC in the experiment would be most problematic. This level was conceived as reasonably implausible. However, the participants' evaluations were on average at the middle of the scale. Thus, users perceive any personal information as essentially learnable from any other personal information the service providers may possess. This perception may indicate learned helplessness, or lost trust in service providers, or general awareness and high sensitivity to the abuse of personal information, or a combination of these factors. Researchers may want to study these perceptions and their antecedents further to find fair, transparent, and efficient solutions that can make such perceptions better reflect reality and can equip users with better control mechanisms. In the meantime, system designers should consider explicitly stating which information can be collected, and which information may become known as a result. Otherwise, regulators and legislators may

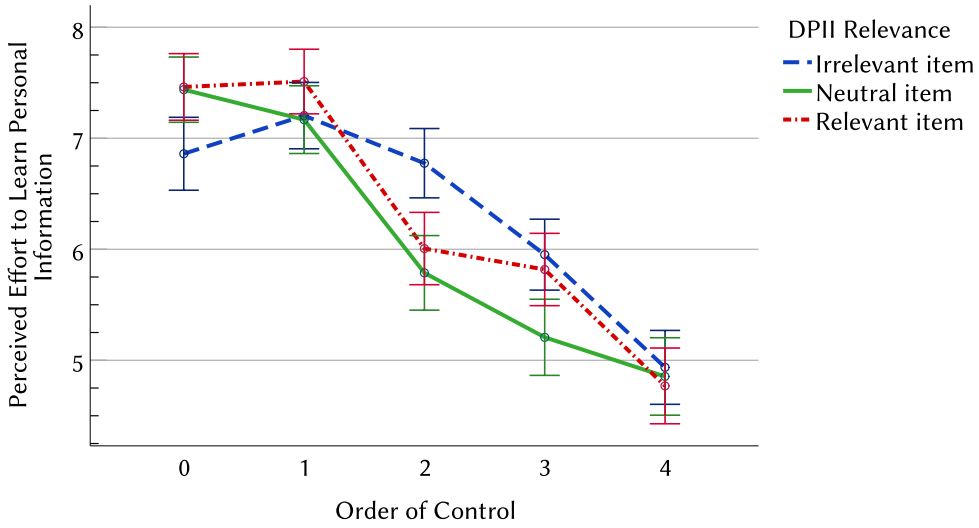


FIGURE 2. Estimated marginal means for the Perceived Effort to Learn Personal Information affected by the *PII Relevance* by the *Order of Control* interaction. Error bars represent 95% CI.

want to consider mandating such a practice, because exercising efficient control is not feasible when the outcomes of disclosures are not clear, be they surely known or apparent.

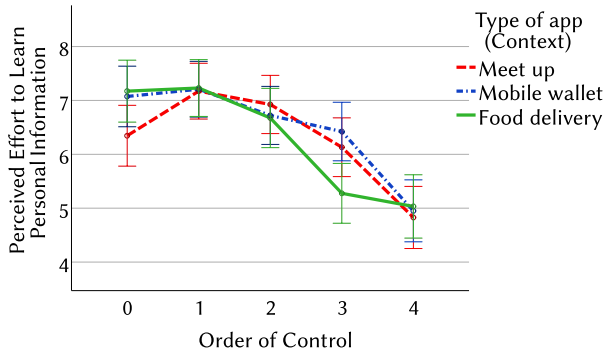
2) ORDER OF CONTROL AND PERSONAL INFORMATION RELEVANCE

The OOC was moderated by the *Relevance* of the personal information items requested by the service providers. Moreover, this combined effect was significant across all three contexts we used in the studies, supporting our second prediction (P2). Even though the way the *Relevance* interacted with the OOC appeared not to be easily interpretable, we concur with the literature on importance of information *Relevance* for user personal information disclosure [39], [40], [42]–[44]. In fact, our findings are in line with [41], demonstrating how *Relevance* has a context-dependent, situational effect, which makes information *Relevance* a significant, yet not systematic, factor of ensuing disclosures. Researchers may be interested in further investigating the effects of *Relevance* in the personal information disclosure processes, aiming to find systematic and consistent, explicable differences. This may make it possible to develop some form of a contextual taxonomy of the information relevance, based on empirical results. Further, more research is needed to understand the mechanism of how the OOC and information relevance interact and affect decisions regarding personal information disclosure. This should be done alongside the study of how the OOC and information relevance relate to other factors, including but not limited to the users' individual characteristics in information processing, level of effort needed to exercise control over personal information disclosure, and actual amount of available control. Additionally, more research is needed to improve our understanding of the subjective perceptions of relevance, as well as its stable and momentary factors. Meanwhile, system designers and privacy practitioners should support transparency of data-processing practices and work to make the relevance of requested information prominent and clear to the users.

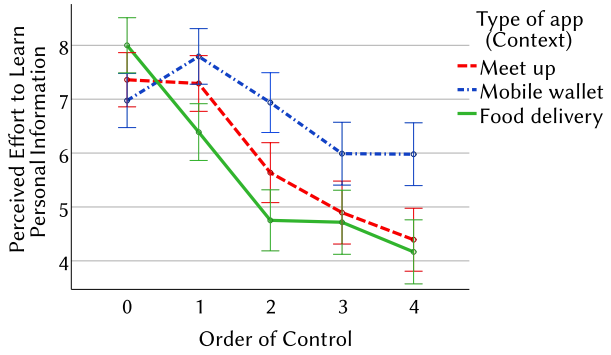
B. LIMITATIONS AND FUTURE RESEARCH

The paper is not without limitations. First, the samples consisted entirely of the English-speaking residents of the USA. We tried to tackle this limitation by not interfering with the sample requirements on the recruiting platform, making the sampling procedure as close to random as possible. We also thoroughly checked the reliability and validity of measurements. Overall, the resulting sample structure and reliability levels should make the findings useful and usable for future research, as well as generalizable to adult populations that are similar to the one in the USA. Another limitation may be relevant for the ecological validity (mundane realism) of the experiment, which relied on vignettes and self-reports. However, both studies included short, not cognitively demanding tasks and were supported by attention-, and seriousness-checks. Methodologically, we also tried to mitigate multiple-treatment interference by randomizing the order of the within-subjects manipulations and their response options. These measures, as well as the free-form feedback we received from the participants, provide us with sufficient confidence in the manipulations and results. The inclusion of the three distinct experimental contexts should make the findings more robust and generalizable.

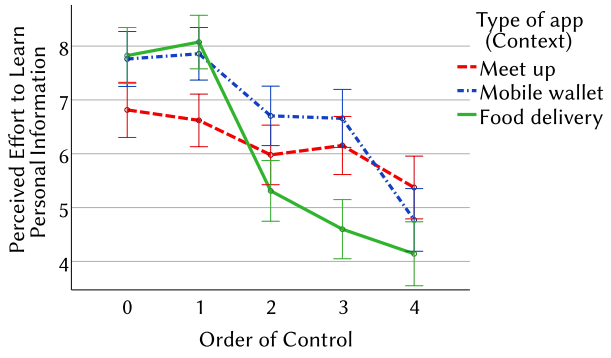
In the preliminary study, more than a half of participants reported to be 60 years of age or older. Prior to making any further analyses, we checked that there were no significant differences in responses regarding the perceived relevance of the PIIs depending on the age cohorts, though the sample structure might have been skewed in terms of experiences with the apps. Even though the age distribution appeared not to have affected the overall results of the preliminary study that were needed for the experiment, it indicated that a deeper focus on the demographics and experiences may be



(a) *Irrelevant* disclosed personal information item



(b) *Neutral* disclosed personal information item



(c) *Relevant* disclosed personal information item

FIGURE 3. Estimated marginal means for the Perceived Effort to Learn Personal Information affected by the *Relevance* and the *Order of Control* across the three *Contexts*. Error bars represent 95% CI.

necessary to better understand the effects of information relevance. Apart from experience with particular apps, privacy literacy can be another contributing multidimensional factor [50], which may be directly or indirectly (e.g., moderated by individual characteristics, such as affect and curiosity [24]) related to the perceptions of control. Establishing an empirical understanding of the perceptions of control as a function of privacy literacy may be able to provide more insight on privacy-related attitudes, as well as to contribute to the study of decision-making regarding personal information disclosure as a whole.[6] Therefore, the demographic characteristics, such as age, gender, and education, as well as experiences, including privacy literacy, should be systematically addressed in future research. Finally, we note that the list of the personal information items used in the studies was neither exhaustive, nor thematic. Future research may benefit from expanding the list by systematically unfolding the categories (e.g., health-related category to include vital signs, physical fitness) or focusing the list on particular themes (e.g., privacy of oneself, privacy of others).

[6]As with any individual characteristics, privacy literacy will need to be addressed using a standardized or at least commonly used instrument (e.g., [51]).

VII. CONCLUSION

This paper offers a conceptual analysis of control over personal information as an approach to better understand such control and find ways to improve it. We introduce the concept of the *Order of Control* as a property of personal information processed by service providers, which demonstrates how perceptions of control decrease when the OOC increases, making information more detached from the users (i.e., the data subjects). Further, we highlight that information *Relevance* plays an instrumental role in perceptions of control. We also show that *Relevance* is subjectively perceived, and confirm that it is context-dependent. We believe this approach can contribute to the study of control over personal information. For instance, it can help develop a measure of effective control to evaluate systems and inform their users, or it can serve as a basis for a control taxonomy, relating actual and perceived control, to inform design and implementation of online systems.

Moreover, the data indicated that users may tend to believe that their personal information can be learned from any other already disclosed data about them, placing any personal information outside of their control. A crucial practical implication is that system designers and privacy practitioners should consider informing the users about information that can become known as a result of other information being disclosed over time. These findings call for further research on perceived control over personal information, studying how users form perceptions and mental models of their ability to control their personal information available to online service providers.

APPENDIX A
PRELIMINARY STUDY: RELEVANCE OF PERSONAL INFORMATION ITEMS IN DIFFERENT CONTEXTS

A. PERSONAL INFORMATION ITEMS

The 34 personal information items presented in the same order to every participant:

1) "Your name".
2) "Your gender".
3) "Your email".
4) "Your phone number".
5) "Your marital status".
6) "Your citizenship(s)".
7) "Your current location".
8) "Where you live".
9) "Your race and ethnicity".

10) "Your sexual orientation".
11) "The events/meetings you are attending".
12) "Your education".
13) "Your job/sources of income".
14) "Your salary/income".
15) "Your bank information".
16) "Your social and economic status".
17) "Your financial situation (e.g., savings, investments, bankruptcy)".
18) "Your purchases".
19) "Your credit history".
20) "Your taxes (payable, returns, etc.)".
21) "Your consumer preferences".
22) "Your interests and hobbies".
23) "Your criminal records".
24) "Information about your relatives".
25) "Information about your friends and colleagues".
26) "Your health status (conditions/diagnoses)".
27) "Your dietary preferences".
28) "Your political opinions".
29) "Your religious beliefs".
30) "Your philosophical beliefs".
31) "Your memberships in, or affiliations with organizations (NGO, church, political action, trade union, club, etc.)".
32) "Your anthropometric information (weight, height, eyesight, physical strength, blood sugar level, etc.)".
33) "Your biometric information (fingerprints, irises, retina, gait, voice, etc.)".
34) "Your genomic data".

B. INSTRUCTIONS FOR PARTICIPANTS

The first page of the instructions read, verbatim:

"Hello and welcome! You are invited to judge for a bit.

In the next pages, we will ask you to consider 3 types of mobile apps, and make judgements about 34 items of personal information in relation to each app. Take as much time as you need and consider them carefully. We would be glad to have your undivided attention to provide your personally most reasonable judgments.

Note: the next pages contain a large table, so it may be more convenient to answer using a desktop or laptop computer rather than a mobile screen."

Next, the participants were instructed on the types of apps and relevance estimation, verbatim:

"Consider the following apps:

- a meet-up app (like MeetMe, Skout, Tinder, Bumble, etc.);
- mobile wallet app (like Google Pay, PayPal, Apple Pay, etc.);
- a food delivery app (in general - any type from any vendor).

We now ask you to classify the personal information items (34 in total) in the Table below into 4 categories, answering the question of How relevant each of the 34 items can be for each of the 3 apps:

1 — The information item is irrelevant for the app (would be suspicious and alerting, if it were requested).
2 — The information item is hardly relevant for the app (would be unusual, if it were requested).
3 — The information item is possibly relevant for the app depending on the goals of collection/processing (would be acceptable, if it were requested).
4 — The information item is relevant for the app to function (would be normal, if it were requested)."

Each of the further pages contained a reminder:

"Considering the same apps, please, keep classifying the information items (*N* out of 34 items left):" *N* depended on the amount of already rated personal information items on previous pages.

C. PARTICIPANTS' DEMOGRAPHICS

Demographic	Level	n	%
Gender	Female	64	58.2
	Male	46	41.8
	Other	0	0.0
	Preferred not to say	0	0.0
Age cohort	18–24	3	2.7
	25–29	4	3.6
	30–34	4	3.6
	35–39	11	10.0
	40–44	7	6.4
	45–49	6	5.5
	50–54	3	2.7
	55–59	9	8.2
	60–64	22	20.0
	65–69	19	17.3
	70–74	15	13.7
	75–79	4	3.6
	80–84	1	0.9
	85–89	1	0.9
	Preferred not to say	1	0.9
Highest completed level of education	Some high school, no diploma	14	12.7
	High school diploma or an equivalent	17	15.5
	Some college credit, no degree	14	12.7
	Trade, technical, vocational training	6	5.5
	Associate's degree or an equivalent	1	0.9
	Bachelor's degree or an equivalent	37	33.6
	Master's degree or an equivalent	19	17.3
	Doctorate degree or an equivalent	1	0.9
	Preferred not to say	1	0.9

APPENDIX B
EXPERIMENT: ORDER OF CONTROL OVER PERSONAL INFORMATION

A. PSYCHOMETRIC SCALE USED IN THE STUDY: PERCEIVED INFORMATION CONTROL

Four items adapted from Dinev *et al.* [22] with minor modifications to item statements to relate to the contexts. The scale reliability was reported in the original paper with $CR(PIC) = 0.92$, $AVE(PIC) = 0.74$, and Cronbach's $\alpha = 0.89$ [22].

1) PARTICIPANT INSTRUCTIONS

Thinking about using [meet up / mobile wallet / food delivery] applications in general to [find social connections / make payments via your mobile phone / get meals and groceries],

please, consider the four following statements carefully for yourself, and indicate to what extent you agree or disagree with these statements.

2) ITEM STATEMENTS

1) I think I have control over what personal information can be released by [meet up / mobile wallet / food delivery] applications.
2) I believe I have control over how personal information can be used by [meet up / mobile wallet / food delivery] applications.
3) I believe I have control over what personal information can be collected by [meet up / mobile wallet / food delivery] applications.
4) I believe I can control my personal information provided to [meet up / mobile wallet / food delivery] applications.

3) RATING SCALE AND ANCHORING

Seven-point Likert-type rating scale anchored verbally: *Strongly disagree – Disagree – Slightly disagree – Neither agree nor disagree – Slightly agree – Agree – Strongly agree*.

B. ANCOVA MODEL EXTENDED BY INCLUSION OF CONTEXT AS A BETWEEN-SUBJECTS FACTOR

Relevance (Rel), Order of Control (OOC), Context (Cxt), and Perceived Information Control (PIC) on Perceived Learnability of Personal Information:

Effect	F	df_{effect}*	df_{error}*	p*	η_p^2
		Within-subjects			
Rel	2.63	1.94	630.62	0.074	0.01
OOC	58.60	2.41	783.12	0.000	0.15
Rel × OOC	3.02	7.58	2462.39	0.003	0.01
Rel × Cxt	4.36	3.88	630.62	0.002	0.03
OOC × Cxt	8.19	4.82	783.12	0.000	0.05
Rel × OOC × Cxt	8.98	15.15	2462.39	0.000	0.05
Rel × PIC	1.18	1.94	630.62	0.307	0.00
OOC × PIC	14.39	2.41	783.12	0.000	0.04
Rel × OOC × PIC	1.03	7.58	2462.39	0.409	0.00
		Between-subjects			
Cxt	3.79	2	325	0.024	0.02
PIC	0.03	1	325	0.855	0.00

* Greenhouse-Geisser corrected for within-subjects effects.

C. PARTICIPANTS' EXPERIENCES

1) FAMILIARITY/USAGE

Question statement read, "Have you been using [meet up / mobile wallet / food delivery] applications? If yes, how many [meet up / mobile wallet / food delivery] applications have you tried so far (approximately, as far as you can remember)?"

Response options:

- Yes, I've used the following number of [meet up / mobile wallet / food delivery] applications: [a field to specify number, response not forced].
- No, I haven't used any [meet up / mobile wallet / food delivery] applications.
- I don't know.
- I don't want to answer.

2) OPEN-ENDED QUESTION

Question statement read, "If you want, please share with us what you think about {[meet up] / [mobile wallet] / [food delivery]} applications." A response would be provided via a free form text box.

REFERENCES

[1] CCPA, DEFINITIONS UNDER. (AB-375). (Jan. 2020). *California Consumer Privacy act of 2018 (CCPA). California Civil Code*. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=2%01720180AB375
[2] "Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation)," *Off. J. Eur. Union*, vol. L119, pp. 1–88, May 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC
[3] I. Altman, "Privacy regulation: Culturally universal or culturally specific?" *J. Social Issues*, vol. 33, no. 3, pp. 66–84, Jul. 1977.
[4] A. Westin, *Privacy and Freedom. 1967*. New York, NY, USA: Atheneum, 1970.
[5] M. A. Clee and R. A. Wicklund, "Consumer behavior and psychological reactance," *J. Consum. Res.*, vol. 6, no. 4, pp. 389–405, Mar. 1980.
[6] T. B. White, "Consumer disclosure and disclosure avoidance: A motivational framework," *J. Consum. Psychol.*, vol. 14, nos. 1–2, pp. 41–51, 2004.
[7] K. D. Martin and P. E. Murphy, "The role of data privacy in marketing," *J. Acad. Marketing Sci.*, vol. 45, no. 2, pp. 135–155, Mar. 2017.
[8] M. Hansen, M. Jensen, and M. Rost, "Protection goals for privacy engineering," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 159–166.
[9] T. Dinev, A. R. McConnell, and H. J. Smith, "Research commentary—Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the 'APCO' box," *Inf. Syst. Res.*, vol. 26, no. 4, pp. 639–655, Dec. 2015.
[10] D. Ariely, "Controlling the information flow: Effects on consumers' decision making and preferences," *J. Consum. Res.*, vol. 27, no. 2, pp. 233–248, Sep. 2000.
[11] K. D. Martin, A. Borah, and R. W. Palmatier, "Data privacy: Effects on customer and firm performance," *J. Marketing*, vol. 81, no. 1, pp. 36–58, Jan. 2017.
[12] J. Gerlach, T. Widjaja, and P. Buxmann, "Handle with care: How online social network providers' privacy policies impact users' information sharing behavior," *J. Strategic Inf. Syst.*, vol. 24, no. 1, pp. 33–43, Mar. 2015.
[13] L. Brandimarte, A. Acquisti, and G. Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social Psychol. Personality Sci.*, vol. 4, no. 3, pp. 340–347, May 2013.
[14] S. Taddei and B. Contena, "Privacy, trust and control: Which relationships with online self-disclosure?" *Comput. Hum. Behav.*, vol. 29, no. 3, pp. 821–826, May 2013.
[15] L. Palen and P. Dourish, "Unpacking 'privacy' for a networked world," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst. (CHI)*, New York, NY, USA: Association for Computing Machinery, 2003, pp. 129–136.
[16] B. K. Judee, "Privacy and communication," *Ann. Int. Commun. Assoc.*, vol. 6, no. 1, pp. 206–249, 1982.
[17] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.
[18] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Comput. Secur.*, vol. 77, pp. 226–261, Aug. 2018.
[19] J. Mosteller and A. Poddar, "To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors," *J. Interact. Marketing*, vol. 39, pp. 27–38, Aug. 2017.

[20] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Inf. Syst. Res.*, vol. 15, no. 4, pp. 336–355, Dec. 2004.
[21] H. Xu, "The effects of self-construal and perceived control on privacy concerns," in *Proc. ICIS 28th Int. Conf. Inf. Syst.*, 2007, pp. 1–14.
[22] T. Dinev, H. Xu, J. H. Smith, and P. Hart, "Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts," *Eur. J. Inf. Syst.*, vol. 22, no. 3, pp. 295–316, May 2013.
[23] D. L. Mothersbaugh, W. K. Foxx, S. E. Beatty, and S. Wang, "Disclosure antecedents in an online service context: The role of sensitivity of information," *J. Service Res.*, vol. 15, no. 1, pp. 76–98, Feb. 2012.
[24] A. Kitkowska, M. Warner, Y. Shulman, E. Wästlund, and L. A. Martucci, "Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect," in *Proc. 16th Symp. Usable Privacy Secur. (SOUPS)*, 2020, pp. 437–456. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/kitkowska
[25] S. Kowalewski, M. Ziefle, H. Ziegeldorf, and K. Wehrle, "Like us on Facebook!—Analyzing user preferences regarding privacy settings in Germany," *Proc. Manuf.*, vol. 3, pp. 815–822, Jan. 2015.
[26] E. Aïmeur, O. Lawani, and K. Dalkir, "When changing the look of privacy policies affects user trust: An experimental study," *Comput. Hum. Behav.*, vol. 58, pp. 368–379, May 2016.
[27] K. Krol and S. Preibusch, "Control versus effort in privacy warnings for webforms," in *Proc. ACM Workshop Privacy Electron. Soc.*, Oct. 2016, pp. 13–23.
[28] A. Kitkowska, Y. Shulman, L. A. Martucci, and E. Wastlund, "Psychological effects and their role in online privacy interactions: A review," *IEEE Access*, vol. 8, pp. 21236–21260, 2020.
[29] B. Zhang and H. Xu, "Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes," in *Proc. 19th ACM Conf. Comput.-Supported Cooperat. Work Social Comput.*, Feb. 2016, pp. 1676–1690.
[30] M. Arcand, J. Nantel, M. Arles-Dufour, and A. Vincent, "The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust," *Online Inf. Rev.*, vol. 31, no. 5, pp. 661–681, Oct. 2007.
[31] C. M. Hoadley, H. Xu, J. J. Lee, and M. B. Rosson, "Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry," *Electron. Commerce Res. Appl.*, vol. 9, no. 1, pp. 50–60, Jan. 2010.
[32] K. J. Aström and R. M. Murray, *Feedback Systems: An Introduction for Scientists Engineers*. Princeton, NJ, USA: Princeton Univ. Press, 2010.
[33] W. Mansell and R. S. Marken, "The origins and future of control theory in psychology," *Rev. Gen. Psychol.*, vol. 19, no. 4, pp. 425–430, Dec. 2015.
[34] R. J. Jagacinski and J. M. Flach, *Control Theory for Humans: Quantitative Approaches to Modeling Performance*. Boca Raton, FL, USA: CRC Press, 2003.
[35] Y. Shulman, T. Ngo, and J. Meyer, *Order of Control and Perceived Control Over Personal Information*. Cham, Switzerland: Springer, 2020, pp. 359–375.
[36] B. G. Southwell, G. Anghelcev, I. Himelboim, and J. Jones, "Translating user control availability into perception: The moderating role of prior experience," *Comput. Hum. Behav.*, vol. 23, no. 1, pp. 554–563, Jan. 2007.
[37] E. Herder and O. van Maaren, "Privacy dashboards: The impact of the type of personal data and user control on trust and perceived risk," in *Proc. Adjunct Publication 28th ACM Conf. User Modeling, Adaptation Personalization*, Jul. 2020, pp. 169–174.
[38] Y. Shulman and J. Meyer, "Is privacy controllable," in *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers*, E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, and S. Krenn, Eds. Cham, Switzerland: Springer, 2019, pp. 222–238.
[39] J. C. Zimmer, R. E. Arsal, M. Al-Marzouq, and V. Grover, "Investigating online information disclosure: Effects of information relevance, trust and risk," *Inf. Manage.*, vol. 47, no. 2, pp. 115–123, Mar. 2010.
[40] H. Li, R. Sarathy, and H. Xu, "Understanding situational online information disclosure as a privacy calculus," *J. Comput. Inf. Syst.*, vol. 51, no. 1, pp. 62–71, 2010.
[41] M. D. Leom, G. Deegan, B. Martini, and J. Boland, "Information disclosure in mobile device: Examining the influence of information relevance and recipient," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2021, p. 4632.
[42] J. L. Hayes, G. Golan, B. Britt, and J. Applequist, "How advertising relevance and consumer—Brand relationship strength limit disclosure effects of native ads on Twitter," *Int. J. Advertising*, vol. 39, no. 1, pp. 131–165, Jan. 2020.
[43] Y.-Q. Zhu and J.-H. Chang, "The key role of relevance in personalized advertisement: Examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions," *Comput. Hum. Behav.*, vol. 65, pp. 442–447, Dec. 2016.
[44] K. D. Sweetser, S. J. Ahn, G. J. Golan, and A. Hochman, "Native advertising as a new public relations tactic," *Amer. Behav. Scientist*, vol. 60, no. 12, pp. 1442–1457, Nov. 2016.
[45] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879–903, 2003.
[46] F. Faul, E. Erdfelder, A.-G. Lang, and A. Buchner, "G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences," *Behav. Res. Methods*, vol. 39, no. 2, pp. 175–191, May 2007.
[47] H. Kaiser, "An index of factorial simplicity," *Psychometrika*, vol. 39, no. 1, pp. 31–36, 1974.
[48] J. Gliem and R. Gliem, "Calculating, interpreting, and reporting cronbach's alpha reliability coefficient for Likert-type scales," in *Proc. Midwest Res. Pract. Conf. Adult, Continuing, Community Educ.*, Jan. 2003, pp. 1–7.
[49] S. W. Greenhouse and S. Geisser, "On methods in the analysis of profile data," *Psychometrika*, vol. 24, no. 2, pp. 95–112, Jun. 1959.
[50] P. K. Masur, "How online privacy literacy supports self-data protection and self-determination in the age of information," *Media Commun.*, vol. 8, no. 2, pp. 258–269, Jun. 2020.
[51] S. Trepte, D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind, *Do People Know About Privacy and Data Protection Strategies? Towards the Online Privacy Literacy Scale (OPLIS)*. Dordrecht, The Netherlands: Springer, 2015, pp. 333–365.

YEFIM SHULMAN received the master's degree in business informatics from the Higher School of Economics, Moscow, Russia. He is currently pursuing the Ph.D. degree with the Department of Industrial Engineering, Tel Aviv University, Tel Aviv, Israel. His research interests include dealing with usable privacy and human–computer interaction, focusing on how to inform user decision-making regarding actions that are consequential for their online privacy and self-presentation.

JOACHIM MEYER (Senior Member, IEEE) received the M.A. degree in psychology and the Ph.D. degree in industrial engineering from the Ben-Gurion University of the Negev, Israel, in 1994. He was a Postdoctoral Fellow and a Researcher at the Technion – Israel Institute of Technology, was on the Faculty of the Ben-Gurion University of the Negev, and was a Visiting Scholar at the Harvard Business School, a Research Scientist at the MIT Center for Transportation Studies, and a Visiting Professor at the MIT MediaLab. He is currently the Celia and Marcos Maus Professor of data science with the Department of Industrial Engineering, Tel Aviv University. He is an Elected Fellow of the Human Factors and Ergonomics Society.