Reciprocities or Incentives? Understanding Privacy Intrusion Perspectives and Sharing Behaviors

Ala Sarah Alaqra & Erik Wästlund

Karlstad University, Karlstad, Sweden
alaaalaq@kau.se

Abstract. The importance and perception of privacy varies from one context to the other. However, everyone values his or her privacy to a certain extent. The subjectivity of that value, attitudes, and behaviors would depend on different entangling factors. It is important to understand the motivation that influences human behavior, whether to protect or share their information. In this paper, we aim at understanding the boundaries of privacy, factors influencing information sharing behavior including experiences (reciprocities of privacy), and efforts taken to protect one's data.

We collected data using quantitative (survey/quiz) and qualitative means (focus groups). In the survey/quiz, our results showed that intrusion experience and awareness have a significant correlation between sharing of data. Furthermore, our focus groups results yielded details on influencing factors for privacy reciprocities and tradeoffs. We discuss our results in terms of privacy incentives and factors influencing the sharing behavior of their information. Finally, we highlight the complexity of behavior where intrinsic and extrinsic motivations could clash and result in a dilemma such as the privacy paradox phenomenon.

Keywords: incentive, reciprocity, privacy, privacy paradox, behavior, motivation

1 Incentives: Motivating Behavior

Understanding human behavior and motivation has been a research goal within different fields. Biologists, psychologists, economists have been exploring human motivation in order to shed a light on understanding decision-making processes. Incentives, used as a motivational technique to stimulate activities and actions, give some insight to prediction modules and strategies [1].

Motivation is generally the reason why people behave in a particular way to achieve their goals, activities, and needs. In psychology, there are two types of motivation: Intrinsic and extrinsic [2], [3]. Intrinsic motivation is related to one's own sense of accomplishment, satisfaction and is closely related to fun, whereas extrinsic motivation is instrumental; dealing with external rewards or consequences [2]. One major theory of motivation is the incentive theory, which focuses on rewards to motivate a behavior.

The *Positive* reinforcement (reward) gives a positive meaning to a behavior, and thus the awarded activity is stimulated to occur repeatedly [4].

Rewards, can have different effects on behavior, possibly unintended, depending on different factors [1].The factor of time (past behavioral influence) has been shown to play an important role in human behavior, and social influence to reciprocity when it comes to incentives [5]. However, human behavior has shown to be more complex than just be motivated by monetary incentives [1], [6]. Studies have emphasized the importance of considering different motives for incentives such as the desire to reciprocate, or avoid social disapproval [7].

2 Privacy: Breaking Boundaries

With the growing online activity, exposure to threats and risks of privacy increases. Apart from cyber adversaries and data collectors, users sharing of their personal information (indirectly or by reciprocity) is a key factor to regulating the intrusion of their privacy.

To define privacy is to select a context and understand which factors and actors are involved in that definition. When considering personal freedom, privacy can be defined as "the right to be let alone" [8]. Whereas context and specific norms are key in the concept of contextual integrity [9].

According to Communication Privacy Management (CPM) theory, people's sharing of private information, using the boundary metaphor, is denoted by boundaries [10], [11]. CMP focuses on the motivations behind people's self-disclosure of their private data using the privacy boundaries. When people keep to themselves, is it considered a *personal* boundary, however when they share information that is when it becomes a *collective* boundary. Understanding when and why these boundaries are crossed is one way to understand sharing behaviors.

When dealing with privacy, especially with human factors, privacy aspects may seem subjective. The tendency to give bias positive responses is higher when it comes to the topic of privacy. The incentive of having the privacy of data being protected is desired and when asked, users tend to agree to that. However, according to the privacy paradox, instances have shown behaviors that entails otherwise. The conflict between attitude, showing concerns and behavior is not new as seen in the works of Barnes, Taddicken and kokolakis [12]–[14]. Privacy paradox show contradictions on users' online behavior, where people would state that they value privacy, however their behaviors might indicate otherwise [12], [13]. It is therefore difficult to tell through empirical research if users are indicating their intention or behavior when it comes to privacy. Hu and Pu compare two preference elicitation methods, the common rating versus personality quiz [15]. They highlight the importance of considering psychological aspects, and indicate that personality quiz could be a powerful tool as alternative to the rating approach for higher accuracy for revealing user's preferences. In the first study, survey/quiz we used a personality test format as a motivational approach by giving users the incentive of "feedback: result of their test", we intentionally avoided monetary incentives due to possible unintended effects [16].

2.1 Scope

In previous research, we have claimed that data privacy is a wicked problem [17], a complex issue with no straightforward solution. An ecosystem of technological, legal, and human factors should be considered when enhancing data privacy. We therefore consider that technological and legal aspects are set, whereas our investigations and contributions of this paper focus on human factors.

The scope of this work is part of the EU H2020 project PRISMACLOUD (Privacy and Security Maintaining Services in the Cloud). The project develops privacy enhancing solutions for avoiding privacy intrusion in the Cloud, such as malleable (redactable) signatures [18]. A malleable signature is a cryptographic scheme that allows specified redaction (removing or blacking out) of fields within a digitally signed document while maintaining the validity of the signature. One of the PRISMACLOUD eHealth use cases allows patients to redact specified fields of documents that were digitally signed by their medical doctor) so that they can share it afterwards. Therefore, it is important to understand user's perspectives as well as which incentives promote their sharing behaviors for the design processes.

2.2 Research Objectives.

In our studies, we investigate attitudes toward privacy incentives and privacy boundaries, and focus on the behavior of sharing personal information and factors that influence their behavior: whether it is reciprocation they seek or an incentive that motivates them. Therefore our research questions are:

- What are the *boundaries* of privacy?
- What factors influence information sharing behavior i.e., which reciprocities are privacy being traded for?
- Can intrusion experiences influence privacy behavior?
- What efforts do users take in order to protect their privacy?

3 Methodologies and Approaches

These studies are part of our Value Sensitive Design (VSD) approach, focusing on the privacy value. VSD approach accounts for human values in comprehensive manner throughout the design process [19]. We also followed User-centered Design approach (UCD) approach in our project, where the focus is on exploring users' perspectives and experiences throughout design processes [20], [21]. We aimed to understand users' online behavior and willingness to disclose "sensitive" information. In specific, what information that is considered private and in which context, how do users perceive intrusions, and what are they willing to do in order to protect their sensitive information from intrusions.

Using empirical methods, we have collected data using both quantitative (survey) and qualitative (focus groups) means in order to investigate, in explorative manner, users' perceptions, and behavior to disclose "sensitive" information. A survey will act

as a quantitative approach; consequently, we investigated and validated results from the survey with focus groups. The following sections will give an account to the two studies' design and procedure.

3.1 Study 1: Survey/Quiz

The survey was conducted online using SurveyGizmo [22]. Choice of the instrument depended on the functionality that permitted the use of personality quiz alternatives. We recruited participants through online forums, brochures around 5 cities in Sweden, contacts mailing lists (In Germany and Italy), and SurveyGizmo sharing option. Aside from English, we had German, Italian and Swedish as alternatives to answer the survey/quiz. We chose Germany, Sweden, and Italy, due to our resources and project partners who aided in translating the survey into corresponding languages

Since privacy is a relatable topic, we targeted all types of possible participants, which made up our convenience sample. We mainly distinct them by enquiring about their technical experience. The survey was online for 6 weeks between March and May 2017.

The survey was calculated (by SurveyGizmo) to take 6-10 minutes to complete. Participants were first given a choice of language: English, Swedish, German, and Italian. Next was the choice to take either a personality quiz or a survey. After that, they were directed to the consent and beginning of the survey/quiz questions, see **Fig. 1**. The questions consisted of 5 sections corresponding to evaluation criteria (see details in section: Questions and evaluation criteria), and feedback and demographic questionnaire which was optional.

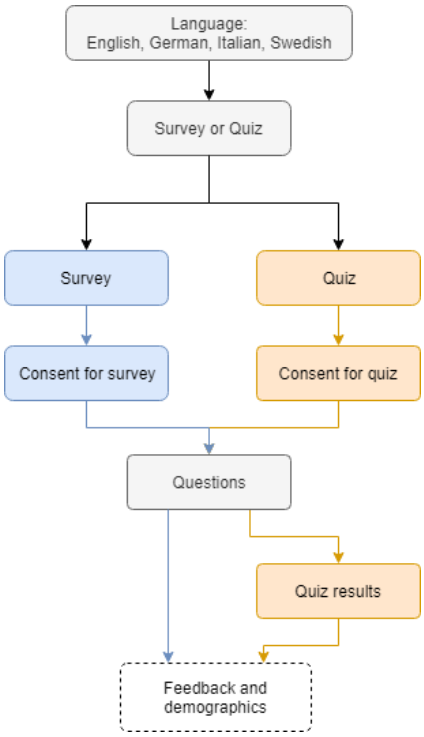

Fig. 1. Flowchart of the survey/quiz

Questions and Evaluation Criteria.

The questions in the survey/quiz were formulated around the context of privacy, however privacy questions were not asked explicitly. Using indirect enquiry, we used daily situations and metaphors to investigate users' perceptions and attitudes. For example, we used situations which could be interpreted as privacy intrusive and asked about them (e.g., being asked about the content of a shopping bag by a random stranger), or online behaviors that they perform (e.g., filling only mandatory fields in forms). The 5 evaluation criteria, described below, correspond to sections in the survey/quiz.

Attitude and Comfort Toward Intrusion.

In this section, there were 5-leveled Likert scale agreement questions varying from "strongly agree" to "strongly disagree". Investigating user's perception of intrusion is crucial in understanding how users perceive privacy. However, how intrusive the behavior may be, it is interesting to investigate the comfort level that users experience when they are put in an intrusive situation. The questions target intrusions to one's information that is more or less private depending on the context and the actors involved. The list of questions describe situations, and subjects are asked to provide feedback by rating their comfort level corresponding to the given situation. The situations

are basically regular activities, e.g., shopping, and then an external actor, e.g., stranger, enquires about unexpected information, e.g., what's in their shopping bag. We expect that most users would feel uncomfortable in such situations, and would be aware of the intrusiveness of the situations.

Experience of Intrusive Situations.

In this section, there were 4-leveled Likert scale frequency questions varying from "never" to "often". Whether users are consciously aware or not of experiences of intrusion, it is interesting to see if they can relate to the scenarios presented. Specifically if they perceive the intrusion of personal information. We are interested to see if familiarity and experience with intrusion situations have an effect on how users behave with their data. Either they are more privacy aware and careful, so that they would prevent future reoccurrences, or they just accept it and don't see any harm in their experience. We expect the former statement, where users become more careful when they have experienced an intrusive situation. In this section, questions were asked if they have experienced (never, few times, several, and many times) similar situations to the same scenarios of previous section.

Sharing of Personal Data and Contexts.

In this section, there were checkbox questions for sharing 5 categories of data in 3 contexts. When addressing personal information, it is difficult to predict what is considered as per se sensitive (independent from the purpose of use) and to what degree for users. We investigated the sharing of personal information of the 5 categories/types of data (medical, political &religious, sexual, income, and demographics) in the contexts of medical staff, employer, and family. The first three listed above categories are regarded as sensitive data according to Art. 9 of the EU General Data Protection Regulation (GDPR), which defines "special categories of personal data" as sensitive for processing [23].

Experience and Effort to Hide Data: Data Minimization.

In this section, there were 5-leveled Likert scale agreement questions varying from "strongly agree" to "strongly disagree". Besides being aware of intrusive situations regarding their personal data, we are interested in their prior experience to limit and hide personal information. The latter would indicate higher privacy value and cautiousness when disclosing information. The questions, regarding information disclosure, enquires if they fill out mandatory fields only in forms, or question the need to provide sensitive information in certain situations. We expect that users, who had experiences with cautious information disclosure, are keener to protect their privacy in the future.

Reciprocity and Privacy.

In this section, there were 5-leveled Likert scale agreement questions varying from "strongly agree" to "strongly disagree". Considering the abovementioned sections, users who are privacy aware are expected to spend more efforts to protect their data's privacy. The corresponding section's questions investigate users' willingness to spend more time, money, effort to enhance their privacy.

The Quiz: Data-introvert or Data-extrovert.

When they began the test, they got a disclaimer stating that the two personas are made-up and not official. Throughout the test, the instrument calculated their answers according to their privacy and sharing responses: when users reach a certain threshold of points they are data-extrovert. After answering all questions, they got instant score and a text describing the result i.e., what does data-introvert means.

3.2 Study 2: Focus Groups

Following the survey, we discussed the research criteria from the survey in depth with focus groups. The qualitative approach allows interactivity and freedom of expression among participants, which allows us to investigate their opinions, perspectives, and attitudes.

Considering the scope of the project involved, we included user groups with different technical background and used the knowledge of digital signature as the selection criteria. When recruiting users, they were asked about their knowledge of digital signatures and to what extent, consequently they were put in either the lay user (no knowledge of how digital signatures work) group or technical group (knowledge of how digital signatures work). We had 5 focus groups (6-7 participants in each) totaling 32 participants in Sweden, Germany, and Norway: 3 lay user groups (FG1, FG3, and FG4), and 2 technical groups (FG2 and FG5).

The focus group sessions consisted of two parts (each lasting approximately 45 mins), since it was combined with another study [24]. The first part was addressing users perspectives on our research criteria from the survey (we also used the results from the survey as input for discussions), which is reported in this paper, and the second part was mock-up discussions (which is not part of this paper). Participants were given consent forms for participating in the study and for recording the sessions. All participants consented to both, and they were urged to not disclose sensitive identifying information (in which case the recording will stop, and the recording section would be deleted). Two researchers at least were in each session, one took notes and the other moderated the discussion.

3.3 Ethical Considerations

To the best of our efforts, the survey/quiz was anonymous. A disclaimer was included in the survey regarding the personality test analysis being fictional (is not a diagnosis), and that is part of our research. No sensitive or personally identifying information was collected, thus complying with the Swedish Ethical Review Act. As for the focus groups, since the recording of voice might be personally identifying data, we submitted it to the Ethical Review Board at Karlstad University, which was approved in May 2017.

4 Findings and Discussions

4.1 Study 1: Survey/Quiz

In total, there were 165 complete and valid responses, where 162 participants filled in the demographics sections, and 111 filled in the feedback section. There was a good distribution of countries and ages as seen in **Fig. 2** and **Fig. 3**. Additionally, we had good distributions of lay and technical users as shown in **Table 1**. Classification of users into Lay and technical depended on their knowledge and experience of two tools: Digital Signatures and Electronic IDs (selection of tools was dependent on our project's scope).

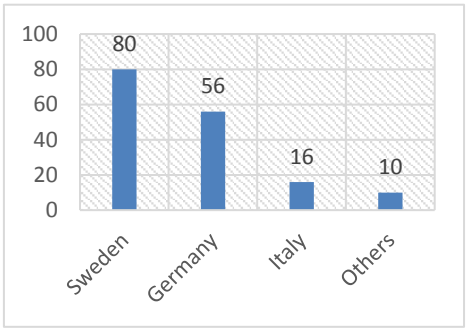

Fig. 2. Demographics showing number of participants in corresponding country

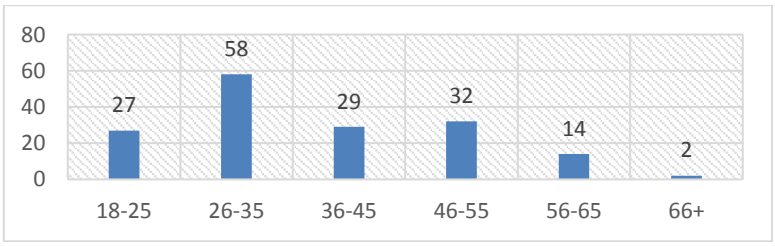

Fig. 3. Demographics showing number of participants in corresponding age-range

Table 1. Demographics showing participants' experience with the two tools as indicators of their technical expertise

Tool /users	Lay	Tech
Electronic ID	60	102
Digital signatures	74	88

In order to investigate the underlying structure of the questions regarding online behavior preferences we conducted a factor analysis (PCA with varimax rotation). The results showed that the questions fell into five factors (see **Table 2**), namely "Intrusion awareness": being consciously aware of the possibility of the intrusion of one's personal information, "Intrusion experience": the personal experience of privacy intrusion, "Effort for privacy tradeoff": willingness to make an effort to protect their privacy, "Privacy for benefits tradeoff": willingness to trade privacy for benefits, and "Data minimization": the ambition to only enter mandatory information. **Table 2** shows the composition of the first to the fifth PCA component, values represent weight of the survey questions in relationship to the factors.

Table 2. The 5 factors and corresponding weights

Rotated Component Matrix	1	2	3	4	5
Data minimization 1			0,702		
Data minimization 2			0,745		
Data minimization 3			0,797		
Privacy for benefits 1			-0,3	0,63	
Privacy for benefits 2				0,725	
Privacy for benefits 3				0,837	
Effort for privacy 1					0,636
Effort for privacy 2					0,695
Effort for privacy 3					0,733
Intrusion awareness 1		0,758			
Intrusion awareness 2		0,713			
Intrusion awareness 3		0,703			
Intrusion awareness 4		0,701			0,324
Intrusion awareness 5		0,671		-0,276	
Intrusion experience 1	0,815				
Intrusion experience 2	0,559				
Intrusion experience 3	0,852				
Intrusion experience 4	0,767				
Intrusion experience 5	0,792				

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

In order to examine to what extent the online behavior preference factors were related to sharing behavior mean scores for each preference factor as well as the sum of all question regarding sharing "Share overall" was calculated for each participant. Pearson correlation coefficients was then calculated between the six variables. The results showed that "Intrusion awareness" and "Intrusion experience" significantly correlated negatively with "Share overall". Additionally, "Effort for privacy" marginally correlated to "Intrusion awareness" (see **Table 3** for r and p values).

Table 3. Sharing behavior and online behavior preference factors

		Share overall	Intrution awareness	Intrution experience	Data minimization	Privacy for benefits	Effort for privacy
Share Overall	Pearson Correlation	1	-,248**	-,286**	-,175*	0,09	0,049
	Sig. (2-tailed)		0,001	0	0,025	0,252	0,531
	N	165	165	165	165	165	165
Intrution awareness	Pearson Correlation	-,248**	1	-0,078	0,093	-0,023	0,152
	Sig. (2-tailed)	0,001		0,316	0,233	0,767	0,052
	N	165	165	165	165	165	165
Intrution experience	Pearson Correlation	-,286**	-0,078	1	0,021	0,081	-0,008
	Sig. (2-tailed)	0	0,316		0,792	0,302	0,918
	N	165	165	165	165	165	165
Data minimization	Pearson Correlation	-,175*	0,093	0,021	1	-0,112	-0,066
	Sig. (2-tailed)	0,025	0,233	0,792		0,151	0,402
	N	165	165	165	165	165	165
Privacy for benefits	Pearson Correlation	0,09	-0,023	0,081	-0,112	1	-0,009
	Sig. (2-tailed)	0,252	0,767	0,302	0,151		0,912
	N	165	165	165	165	165	165
Effort for privacy	Pearson Correlation	0,049	0,152	-0,008	-0,066	-0,009	1
	Sig. (2-tailed)	0,531	0,052	0,918	0,402	0,912	
	N	165	165	165	165	165	165

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

To further investigate perceptions of sensitivity of the data types and their willingness to share data we looked at the distribution of participants who were willing to share vs those who were not willing to share. The results showed that perceptions of sensitivity spanned form very sensitive "sexual data" to not sensitive at all "Demographics" (see **Fig. 4** for proportions of willingness to share different datatypes).

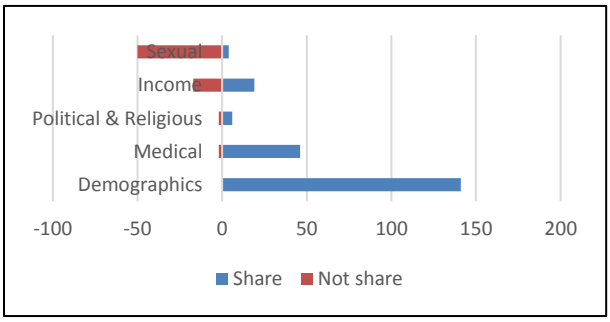

Fig. 4. Willingness to share different datatypes

To follow up on the perceptions of sensitivity of the different datatypes we looked at the specificity of contexts (medical, employer, family) where the datatypes were shared. This was done by calculating the number of different contexts where the

datatypes were shared[1]. The results showed that again "Demographics" was the least sensitive datatype as this was shared among **all three contexts by** 85% of participants whereas "Political and Religious" was the most sensitive insofar that it was only shared within **one context** by 88% percent of participants (see **Table 4.** Willingness to share with up to 3 different contexts).

Table 4. Willingness to share with up to 3 different contexts

	Number of contexts		
Type of data	1	2	3
Demographics	3,05%	10,98%	85,98%
Income	45,95%	41,22%	12,84%
Medical	12,27%	59,51%	28,22%
Political & Religious	88,28%	7,59%	4,14%
Sexual	66,96%	29,57%	3,48%

4.2 Study 2: Focus Groups

In the discussions of focus groups, all groups shared the opinion regarding the sensitivity of medical, political, sexual, religious, and income data. Most indicated that they would not share sensitive data, whereas they are willing to share demographic data such as age, profession, address.

Sharing Behavior and Factors.
Since we were interested in understanding the sharing behavior of the participants, we asked of situations and factors that they see themselves sharing more or less information than they already have. **Table 5** summarizes the results of influencing factors to sharing information by the focus groups and shows the distribution of both user types, details of the factors are provided below.

1. Context refers to the environment where participants are sharing information in. For instance, on online dating site, one would reveal different type of information than their professional profile on the web. Additionally, if one is engaging in a specific context e.g., political discussion, then they would have directly/indirectly reveal their political affiliation, which they consider sensitive information.
2. Peer-pressure is the obligation to share certain information due to social pressure: e.g., everyone has shared a piece of information, or due to norms that pressure one to provide some information about one's self.
3. Social acceptance/appeal is wanting to bond with others by sharing information and details based on common grounds and wanting to be liked by others.

[1] The calculations of the proportions of number of contexts is based on those who were willing to share.

4. Duration of interaction refers to time spent with someone, e.g., the feeling of comfort and familiarity will allow sharing more information with the person you have spent more time with.
5. Face to face or offline interaction allows more sharing of information than online, where one lacks control and certainty of whom they are sharing information with and if information is stored somewhere online.
6. Not documented or recorded conversations allows freedom of revealing personal information, whereas one might be more careful in revealing information about themselves in recorded conversations.
7. One on one is more intimate and trustworthy environment to share information than a setting containing a group of people, where one would not feel comfortable sharing with everyone in the group.
8. Experience with age refers to how older generation tend to be more private about their information and sharing behavior/online activity seem to differ from their children.
9. Prior bad experiences tend to make one more cautious when sharing information, since it can also become a personality trait of being more private.
10. Consequences concerns of sharing personal information, especially with health data, could lead to problems such as insurance conflicts. Another concern is profiling through revealing data that is not secretive. Also metadata or derived sensitive information that one is not willing to share.
11. Cultural influences refers to a cultural/social stance on some information that is considered private, e.g., sharing income data in Germany is considered a taboo and thus no one would share that type of data.

Table 5. Factors affecting sharing behavior among lay and technical participants: more (+), more vs. less (+/-), and less (-)

No.	Factor affecting sharing behaviors	Lay	Tech.
1.	Context	+	+
2.	Peer-pressure/norms	+	+
3.	Social acceptance/appeal		+
4.	Duration of interaction	+	
5.	Face to face vs. online	+/-	+/-
6.	Not documented vs. recorded		+/-
7.	One on one vs. groups	+/-	+/-
8.	Experience with age	-	
9.	Prior bad experiences	-	
10.	Consequences concerns: profiling, metadata	-	-
11.	Cultural influences	-	-

Efforts to Protect/Hide Information.

In the discussion about the willingness of participants to protect or hide their data and what efforts they undertake, many indicated that they actively try to limit their

exposure. Means and efforts mentioned by participants (lay and technical) are clustered into the three following categories.

Rejection the Use of Services.

Participants indicated that they would not use the following services for privacy and security reasons. They stated that it is part of their efforts to protect their data's privacy.

- Social media ,e.g., Facebook, WhatsApp (lay and tech)
- Free services, e.g., public Wi-Fi (lay and tech)
- Cloud services, e.g., storing photos (lay)

Limitation of Information Exposure.

According to participants, one way to protect their data is to limit their exposure to privacy intrusive possible portals. Limiting the exposure of one's information online by using ad-blocks for browsing online, or controls to limit online access and sharing of data, and paying for avoiding customized advertisements.

- Using Ad-blocks (lay)
- Controls for online exposure, e.g., sharing pictures (tech)
- Using cash for anonymity (lay)
- Using fake emails (tech)
- Paying for services: Wi-Fi, non-Ad Apps (tech)

Taking on Inconvenient Alternatives.

Another approach was to find alternatives for limiting one's possible exposure, however it was noted that not many alternatives exist, and the current ones are inconvenient/cumbersome. Many indicated that they would try to use alternative services that are more privacy friendly, or that they would implement their own service to ensure they have more control.

- SMS instead of chats that require profiles (lay)
- non-smart phone for communication (lay)
- Offline shopping, avoiding ads (lay)
- Using own domain for emails (tech)
- Implement own service (tech)

4.3 Discussions

Privacy Boundaries, Attitudes, and Experience.

According to our results, participants showed more or less reservation regarding sharing information, which indicated their boundaries of privacy. In the focus groups, many indicated further reservations in normal settings (outside the context of a focus group discussion where they share their opinions and experiences). Our discussions mainly focused on voluntary self-disclosure (sharing information and crossing the privacy boundary willingly), thus excluding external enforcements of disclosure e.g., law

enforcement. The value of having one's data being private (personal boundary) holds true for many especially when they have control over it (voluntary disclosure).

However, participants indicated that they would share more or less information depending on the type of data, which varies in sensitivity; that sensitivity is confirmed by both studies to be affected by the context the information is being shared in. For example, the case of declaring political affiliation as sensitive data, yet revealing that information in a political discussion. This indicates that privacy is situational, and exchange of information is a balance between risks and benefits at that specific point [6]. Experiences and privacy awareness significantly correlated to sharing behavior in our survey/quiz. Similarly, in the focus groups, participants indicated experience with age and bad experiences are factors for having concern to sharing information. However, despite having a privacy-concerned attitude, that does not ensure privacy correct perception or behavior. In the work of Joinson et al. [25], where they addressed the relationship between privacy concerns and users disclosure (behavior) online. They concluded that privacy concerns do not necessary influence the perception of privacy-related situation.

Privacy: Incentives and Reciprocities.

From the 5 factors of the survey/quiz, there was a distinction between: "Effort for privacy tradeoff": willingness to make an effort to protect their privacy and "Privacy for benefits tradeoff": willingness to trade privacy for benefits. While in many cases there are efforts to protect and enhance privacy, there are also instances where privacy is being traded for other benefits. Consequently, indicating that privacy is not necessary the most important incentive at all times. The voluntary act of sharing one's information was discussed in the focus groups, and reciprocity was key factor in sharing information. That happens when one is trading their privacy for other benefits (intrinsic and/or extrinsic) such as social acceptance and likability, engaging and interacting, and performing certain settings (context).

Influencing factors to sharing information, mentioned in the focus groups, contained both intrinsic and extrinsic values. While in many cases the values were directly associated with the benefit, the complexity of sharing information was further highlighted in the focus groups. Some participants mentioned that they chose to share more information online to mitigate false profiling, thus by sharing correct information about themselves, they control how they are profiled online. Also, a couple of participants indicated that hiding information might be perceived as suspicious and thus chose to share information in certain occasions consequently to avoid false image. The above-mentioned instances show behaviors of sharing more information because of limited control over the environment and fearing consequences of protecting their own privacy. The contradiction in behavior (sharing information) and situation is an instance where extrinsic (the situation) and intrinsic (privacy-aware) values are mismatching thus affecting the behavior.

Similarly, related work by Li et.al addressed the entanglement of information as non-independent activity from other happenings [6]. In their study, they addressed the sharing of information as secondary exchange to a primary online shopping exchange. Fairness and relatedness of information has shown to be important factor to the information

exchange. They also showed that monetary incentive (extrinsic value) could have undermining effects on user's willingness to share information if the information is not relevant.

Discussions in the focus groups revealed a general attitude for having high regard to privacy, however only some active efforts to protect one's privacy were mentioned. The main issue highlighted was that despite the acknowledgement of one's privacy being important, it fades when other incentives or needs are present, thus trading one's privacy in reciprocity for a service or functionality. Additionally, all the mentioned efforts were perceived as inconvenient and the lack of suitable and usable alternatives was a major issue. This indicates that efforts to protect one's privacy are hindered by the lack of suitable alternatives and not only attitudes; also, they fall short depending on the situation and needs.

Limitations.

Due to our empirical research, one main limitation is the sample size and scope. We had only the countries involved in our both studies limited to our available resources, and lacked international representatives of the sample. However since the research is explorative, this could act as starting point to expand the study and perform some comparative study with regions outside the European Union, where rules and regulations differ and might influence voluntary sharing of information.

5 Conclusions

Privacy has always been regarded as important, whether it is a personal freedom, right, or preference. However, it is not always the most important incentive, which explains why human behavior, as in the privacy paradox, contradicts to privacy concerns. External influences and other factors are contributing to the perceived privacy unfriendly behaviors. Future solutions should consider providing alternatives to existing incentives that are being traded for one's privacy. Reciprocity is key when addressing privacy behaviors and considerations for different influencing factors are crucial for future research and applications.

Acknowledgements. This work is supported by the EU Horizon 2020 research project № 644962 PRISMACLOUD "Privacy and security maintaining services in the Cloud". We extend our thanks to Simone Fischer-Hübner for her valuable input, our project partners who aided our studies, and to the volunteers who contributed to this research.

References

1. E. Kamenica, "Behavioral Economics and Psychology of Incentives," *Annu. Rev. Econ.*, vol. 4, no. 1, pp. 427–452, Aug. 2011.
2. R. M. Ryan and E. L. Deci, "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions," *Contemp. Educ. Psychol.*, vol. 25, no. 1, pp. 54–67, Jan. 2000.

3. R. J. Vallerand, “Toward A Hierarchical Model of Intrinsic and Extrinsic Motivation,” in *Advances in Experimental Social Psychology*, vol. 29, M. P. Zanna, Ed. Academic Press, 1997, pp. 271–360.
4. P. R. Killeen, “Incentive theory,” *Nebr. Symp. Motiv.*, vol. 29, pp. 169–216, 1981.
5. J. André, “The Evolution of Reciprocity: Social Types or Social Incentives?,” *Am. Nat.*, vol. 175, no. 2, pp. 197–210, Feb. 2010.
6. 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.
7. E. Fehr and A. Falk, “Psychological foundations of incentives,” *Eur. Econ. Rev.*, vol. 46, no. 4, pp. 687–724, May 2002.
8. S. D. Warren and L. D. Brandeis, “The right to privacy,” *Harv. Law Rev.*, pp. 193–220, 1890.
9. H. Nissenbaum, “Privacy as contextual integrity,” *Wash Rev*, vol. 79, p. 119, 2004.
10. S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure*. SUNY Press, 2012.
11. S. PETRONIO, N. ELLEMERS, H. GILES, and C. GALLOIS, “(Mis)communicating Across Boundaries: Interpersonal and Intergroup Considerations,” *Commun. Res.*, vol. 25, no. 6, pp. 571–595, Dec. 1998.
12. S. Kokolakis, “Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon,” *Comput. Secur.*, vol. 64, pp. 122–134, Jan. 2017.
13. S. B. Barnes, “A privacy paradox: Social networking in the United States,” *First Monday*, vol. 11, no. 9, Sep. 2006.
14. M. Taddicken, “The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure,” *J. Comput.-Mediat. Commun.*, vol. 19, no. 2, pp. 248–273, Jan. 2014.
15. R. Hu and P. Pu, “A comparative user study on rating vs. personality quiz based preference elicitation methods,” in *Proceedings of the 14th international conference on Intelligent user interfaces*, 2009, pp. 367–372.
16. B. C. Tietje, “When do rewards have enhancement effects? An availability valence approach,” *J. Consum. Psychol.*, vol. 12, no. 4, pp. 363–373, 2002.
17. A. S. Alaqra, “The Wicked Problem of Privacy : Design Challenge for Crypto-based Solutions,” 2018.
18. M. Chase, M. Kohlweiss, A. Lysyanskaya, and S. Meiklejohn, “Malleable Signatures: Complex Unary Transformations and Delegatable Anonymous Credentials.,” *IACR Cryptol. EPrint Arch.*, vol. 2013, p. 179, 2013.
19. B. Friedman, P. H. Kahn, and Jr., “Value Sensitive Design: Theory and Methods,” 2002.
20. N. S. Anderson, D. A. Norman, and S. W. Draper, “User Centered System Design: New Perspectives on Human-Computer Interaction,” *Am. J. Psychol.*, vol. 101, no. 1, p. 148, 1988.
21. C. Abras, D. Maloney-krichmar, and J. Preece, “User-Centered Design,” in *In Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*, 2004.
22. K. Rattray, “SurveyGizmo | Enterprise Online Survey Software & Tools,” *SurveyGizmo*. [Online]. Available: https://www.surveygizmo.com/. [Accessed: 11-Feb-2019].
23. N. Vollmer, “Article 9 EU General Data Protection Regulation (EU-GDPR),” 05-Sep-2018. [Online]. Available: http://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm. [Accessed: 13-Feb-2019].
24. A. S. Alaqra, S. Fischer-Hübner, and E. Framner, “Enhancing Privacy Controls for Patients via a Selective Authentic Electronic Health Record Exchange Service: Qualitative Study of

Perspectives by Medical Professionals and Patients," *J. Med. Internet Res.*, vol. 20, no. 12, p. e10954, 2018.
25. A. N. Joinson, U.-D. Reips, T. Buchanan, and C. B. P. Schofield, "Privacy, Trust, and Self-Disclosure Online," *Human–Computer Interact.*, vol. 25, no. 1, pp. 1–24, Feb. 2010.