An open door may tempt a saint: Examining situational and individual determinants of privacy-invading behavior

Markus Langer, *Saarland University;* Rudolf Siegel and Michael Schilling, *CISPA Helmholtz Center for Information Security;* Tim Hunsicker and Cornelius J. König, *Saarland University*

https://www.usenix.org/conference/soups2022/presentation/langer

This paper is included in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

An open door may tempt a saint: Examining situational and individual determinants of privacy-invading behavior

Markus Langer[§], Rudolf Siegel[*], Michael Schilling[*], Tim Hunsicker[§], Cornelius J. König[§]

[§] Saarland University, Industrial and Organizational Psychology, Saarbrücken, Germany

[*] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

The first two authors contributed equally to the article (shared first authorship)

Abstract

Digital life enables situations where people invade other's privacy – sometimes with harmful intentions but often also without such. Given negative effects on victims of privacy invasions, research has examined technical options to prevent privacy-invading behavior (PIB). However, little is known about the sociotechnical environment where PIB occurs. Therefore, our study ($N = 95$) examined possible situational (effort necessary to invade privacy) and individual determinants (e.g., personality) of PIB in a three-phase experiment. 1) Laboratory phase: participants were immersed into the scenario; 2) privacy-invasion-phase at home: automatically and covertly capturing participants' PIB; 3) debriefing-phase at home: capturing whether participants admit PIB. Our results contribute to understanding the sociotechnical environment in which PIB occurs showing that most participants engaged in PIB, that the likelihood of PIB increased when it required less effort, that participants less likely admitted PIB for more sensitive information, and that individual characteristics affected whether participants admitted PIB. We discuss implications for privacy research and design.

1 Introduction

Everyday, people provide private information in digital spaces. This way, we reveal information that attracts the attention of companies, governments, but also of people in our every day's life [1]. For example, we might observe somebody else's smartphone conversations while sitting in the bus (i.e., "shoulder surfing"; [2]). Sometimes it may be tempting to look into someone's browser history when they have left their device unattended [3] or to read an email that has accidentally been sent to the wrong recipient [4]. These examples describe behavior where people access private information of others – not necessarily to do any harm but due to curiosity [2]. We subsume this behavior under the term privacy-invading behavior (PIB).

Although PIB may not be intended to harm anyone, it seems to be socially unacceptable and can lead to negative consequences [2, 5]. Specifically, PIB evokes negative feelings for people whose privacy is being invaded (e.g., feeling observed, harassed; [5]). Furthermore, experiences with PIB can crucially affect future social interactions or handling of sensitive information [6, 7] (e.g., stop using social media; remain overcautious in digital communication). Although for people engaging in PIB it can come with positive feelings such as amusement, they can also end up feeling uneasy or guilty [2].

PIB happens frequently [2] but research knows little about *when* such behavior becomes more likely and about *who* will be more likely to engage in such behavior. Moreover, to the best of our knowledge what we know stems from correlative research which is understandable given the possible ethical issues associated with experimental intervention studies. To overcome this limitation and to shed further light on situational and individual characteristics that determine PIB in digital spaces, we conducted an experimental study including three phases in a highly controlled but nevertheless realistic setting enabling to control ethical issues associated with this kind of research. In phase 1, participants were asked to provide private information about themselves in a laboratory study. In this phase, participants also responded to questionnaires capturing individual characteristics (e.g., personality). In phase 2, participants received an email including private information captured in phase 1 from a supposed other participant (a text and a video file). This way, participants were given the opportunity to show PIB by accessing information of the other person. We manipulated the "necessary effort" to access these information: Whereas one half of participants was able to access the information directly via a link, the other half needed to insert a password that was easy to guess. Access of the files was tracked. In phase 3, participants received another email telling them that there has been an error during the sending of emails in phase 2. Then, they were asked to indicate whether they accessed the files and were asked to justify their possible PIB. With these three phases, it was possible to show a) that most participants engaged in PIB (66% accessed the text, 57% the video file), b) that situational characteristics (i.e., necessary effort) influenced the likelihood that people invade others' privacy, c) that individual characteristics captured in phase 1 negligibly affected whether people invade other's privacy in phase 2, and d) that the type of information as well as individual characteristics influenced whether people admitted that they accessed other's private information. Our study contributes to our understanding of PIB by shedding light on sociotechnical environments that may promote or prevent PIB.

2 Related Work

2.1 Privacy-invading behavior

Research has investigated PIB predominantly from the perspective of deliberate attacks and with the goal to prevent privacy invasions. For instance, Bošnjak and Brumen [8] reviewed research on ways to prevent harmful privacy invasion through shoulder surfing. Shoulder surfing describes behavior where people covertly observe somebody else's screen of those people's electronic devices [2]. This way, observers can access sensitive data and the victim can be harmed (e.g., by finding out someone's passwords; [9]). As another example of PIB, in an infamous incident, employees at a company selling security cameras had access to customers' cameras for administrative or maintenance reasons but also occasionally accessed camera recordings for other reasons thus invading those people's privacy [10]. Even though some of the aforementioned behavior could be aimed towards harming someone (e.g., blackmailing; voyeurism; [11]), PIB also happens without any intention to harm. Results by Eiband et al. [2] as well as research on social curiosity [12–14] support that PIB is often not aimed towards harming anyone. When people engage in shoulder surfing, they often do so with harmless intentions, and due to curiosity and boredom [2]. Accordingly research sometimes distinguishes PIP according to whether it was intentional (vs. unintentional) and according to the nature of the consequences for the victim (harmful vs. non-harmful) [15]. Following this classification, our study addresses unintended PIB with non-harmful consequences. In our opinion, however, the classification of PIB in such a scheme lacks objectivity and may therefore fall short of the mark: Even though PIB might be without any harmful intent, people might later start to use the collected information in a harmful way. For example, pupils might make fun of another pupil because of watching a video they deem to be "uncool". Collecting this information by shoulder surfing might have happened without a certain intention but results in negative consequences. In addition, even if a certain information is not used in a harmful way, the person whose privacy is invaded may still feel attacked or angry because someone accessed information without consent. Thus, even benign PIB without intent may result in negative consequences for the victim.

2.2 Determinants of PIB

Even without harmful intentions, PIB can involve negative consequences for people whose privacy is being invaded. To prevent such negative outcomes, it is crucial to understand such behavior and to prevent privacy invasions. Whereas technical means to hinder PIB are one important factor [8], examining why people engage in such behavior helps to better understand sociotechnical environments that affect PIB [2].

Initial work has investigated the determinants of PIB. In this regard, Eiband et al. [2] was the main inspiration for the current study. They used a survey to understand the situations where shoulder surfing happens and to investigate motivations that may determine shoulder surfing. From their results, we identified two possible categories of determinants of PIB: 1) situational determinants, 2) individual characteristics. However, the results by Eiband et al. [2] stemmed from a survey where participants reflected situations where they engaged in PIB in the past, only allowing for post-hoc interpretations of possible determinants of PIB. We aimed to go beyond these results and examine the hypothesis that situational and individual determinants affect PIB by experimentally investigating their possible effects.

Regarding situational determinants, arguably there is a large variety of situational determinants that may affect PIB. In line with the findings by Eiband et al. [2] we focus on *effort to access private information*. Their participants reported that other people's electronic devices were in their line of sight which made them inadvertently watch other people's interaction on their devices. Consequently, in this situation PIB may happen because people do not need to take efforts to engage in behavior that allows them to access private information. In digital environments, passwords are one example to make it more effortful to access someone's private information. Uploading files into a shared cloud and using a password for these files increases the effort necessary to access this information. This is also true if the password is easily available (e.g., because it is written down in another file) or guessable (because the password is the other persons' date of birth, which is still often the case; [16]).

In our study, we experimentally manipulated whether more effort was necessary to access someone's private information. Specifically, participants in our study received an email that was clearly addressed to a different person. In one condition, private information was password-encrypted (with the possibility to derive the password from the information available in the email). Participants thus needed to find out the password, type in the password, and only then had access to private information of the other person – they needed to show effort before they could access private information. In contrast, in the no-password condition, participants had to click on a link to readily access the private information. In line with this argumentation, we propose the following hypothesis:

Hypothesis 1: Participants show more PIB when accessing the private information requires less (i.e., clicking on a link) compared to more effort (entering a password that participants need to derive from an email).

Beyond situational determinants, individual characteristics may influence the likelihood that people engage in PIB. Prior research suggested that a large range of individual characteristics could affect PIB [2, 14]. We thus focus on a range of individual characteristics that can roughly be put into three groups: personality, privacy concerns, and individual characteristics that align with possible motivations behind PIB.

Under personality we subsume the Big Five personality facets openness for experience, conscientiousness, extraversion, agreeableness, and neuroticism [17], honesty-humility as proposed to be the sixth general personality facet [18], as well as the three dark personality facets Machiavellianism, narcissism, and psychopathy [19]. People with a high openness for experience enjoy new activities [20], thus they may also be more interested in acquiring private information of others. Highly conscientious people take obligations seriously [21] and see possibly harmful behavior as more problematic [22]. Thus, they may be less likely to invade other's privacy. Extroverted people are sociable and enjoy getting to know others [21]. Research has shown that introverted people value privacy more strongly which also seems to apply to digital privacy (e.g., they share less information online; [23]). Consequently, it might be less likely that introverted people will invade others privacy. Agreeable people tend to shun away from confrontation and want to get along with others [18]. For them, PIB may be less likely because privacy invasions may offend others. People high on neuroticism worry about many things and are more easily to upset [21]. They have been found to be especially concerned about sharing sensitive information [22] thus they might also be less likely to take a look at sensitive information of others. Honesty-humility describes a personality facet of people who are honest and who tend to follow rules [18]. People with high levels of honesty-humility may be less likely to engage in PIB because it constitutes behavior that contradicts the rules of good citizens' behavior.

Dark personality facets subsume Machiavellianism, narcissism, and psychopathy [19]. All of these traits may increase the likelihood that people will engage in PIB. Machiavellianism describes a trait of people who use cunning methods to manipulate others to their own benefit and who have little emotional involvement in interpersonal relations. People high on Machiavellianism have been found to disrespect others' privacy [24, 25] and may thus also be more likely to show PIB. Narcissism reflects a trait of people who believe they are more important than others and who want to be admired. People with strong narcissistic personality tend to disclose more private information on social media [23] and might be more likely to invade other's privacy because they want to compare themselves to others [19]. People with high levels of psychopathy lack empathy and remorse and are less concerned with morality of their actions [19]. They may thus be more likely to invade other's privacy because they may not realize that this is uncomfortable for the person whose privacy is being invaded.

Privacy concerns might additionally be an important determinant of individuals' PIB. People with strong privacy concerns are sensitive about their private data and more generally about the topic of privacy [7, 26]. Consequently, such people may be less likely to engage in PIB as they are more aware of the sensitivity of private information. Furthermore, they may less likely access others private information because they themselves would not want their privacy to be invaded.

Finally, we hypothesize that people with tendencies for online exhibitionism, thrill-seeking, and social curiosity (i.e., individual characteristics that align with possible motivations behind PIB) make PIB more likely. Online exhibitionism describes a characteristic of people who enjoy presenting themselves on the internet [27]. As people who engage in online exhibitionism reveal much private information, they might also be more interested in other's private information. Thrill-seekers are people who like to engage in dangerous and semi-legal activities for the sake of experiencing novelty [13]. Thrill-seekers may enjoy that they are engaging in unaccepted behavior thus being more likely to invade others privacy. Finally, social curiosity describes a characteristic of people who are interested in the lives of other people, but in extreme versions can also be a characteristic of people who enjoy observing others without their knowledge [14]. This indicates that social curious people may be more likely to invade other's privacy.

In sum, for all these individual characteristics, there is reason to believe that they can influence PIB. We thus propose the following research question (RQ):

RQ1: Do individual characteristics affect the likelihood of PIB?

2.3 Admitting PIB

Since PIB is socially unacceptable and associated with negative consequences for the parties involved [2, 5], admitting such behavior might not be easy and may depend on situational and individual characteristics. Regarding situational determinants, if it required more effort to access someone's private information, wrongdoing may be more salient and it might be less plausible to deny it. In our case, if participants only need to click on a link, they can admit that they did so because they can plausibly say it happened because they wanted to check what kind of information are provided behind these links. However, if people have to find out a password, type in this password and thus take effort to access the provided information, it is less plausible to deny that they accessed private information "by accident". Thus, these people may be less likely to admit that they accessed private information due to being aware of their wrongdoing.

Hypothesis 2: Participants will less likely admit PIB when accessing the private information requires less compared to more effort.

Regarding individual characteristics, some of the aforementioned characteristics may increase the likelihood that people admit that they engaged in PIB, whereas others may make it less likely. Specifically, conscientiousness, agreeableness, and honesty-humility may increase the likelihood that people admit wrongdoing. In contrast, the dark personality facets may decrease this likelihood. For the other individual characteristics we capture in our study, it is less straightforward to propose associations with admitting PIB. However, to explore the relation of individual determinants and admitting PIB we propose,

RQ2: Do individual characteristics affect the rate with which people admit PIB?

3 Method

Following suggestions to prevent typical fallacies of non-reproducible science [28], we preregistered our hypotheses and research questions, dependent variables that we wanted to capture, experimental manipulations, data analysis plan, and planned number of participants before data collection started. While conducting the experiment and the analyses, we followed our preregistration available at https://aspredicted.org/e4m32.pdf. The materials, data, and analysis to reproduce the current findings are available at https://osf.io/zcq2e.

3.1 Ethics statement

The first authors' university's ethical review board evaluated and approved this research project. Since this study included deception, a complex design, and a sensitive context, a requirement for ethics approval was a controlled environment that enabled managing participant flow, ensuring that participants do not reveal the purpose of the study to others, and ensuring that participants are contactable for debriefing. This was only possible with a student sample. To enable informed consent, we debriefed participants about the study objective, informed that participation was voluntary and highlighted repeatedly that participants could withdraw from the study. Further, we did not collect any personally identifiable information, and none of the authors were instructors of the student participants to ensure voluntariness. The evaluation materials that were sent to the participants were created together with a professional actress. At the end of phase 3, we conducted a formal debriefing for participants, informing them of the true purpose of this study and assuring them that no personal information was stored from them.

3.2 Procedure

The study consisted of three phases. In phase 1, participants took part in job interview study in a laboratory setting which served as the cover story for our study. In phase 2 (one day after phase 1), participants received an email with the experimental manipulation. In phase 3 (two days after phase 2), there was a post-experimental survey. Figure 2 shows a flow chart summarizing the study procedure.

3.2.1 Phase 1: Laboratory examination

Participants were invited to our laboratory and were told that they will conduct a study on the automatic evaluation of job interviews. After giving their informed consent, participants were asked to complete a questionnaire capturing demographic data and individual characteristics (see section 3.3). Then, they participated in a mock job interview with a trained interviewer. During the interview, a video camera filmed participants, and they were able to see that a video recording software recorded them on a nearby computer monitor. This was done to ensure that participants believed that they were recorded during the interview and later automatically assessed by a computer program (however, we never actually recorded the interviews). The interview started with common questions (e.g., tell us about your strengths) and continued with increasingly personal questions (for instance asking about participants' family planning, marital status; we chose questions that are illegal in selection interviews but where research has shown that they are common in practice [29]). To increase plausibility of our cover-story, after the interview, participants responded to questions assessing their perception of the interview process (e.g., regarding fairness of the process; [30]). However, the only purpose of the interview was to draw attention to the interview setting and to make participants believe that they, and other participants who would take part in the study, had to share private information with the interviewer and that this information was recorded. In the end of phase 1, participants were told that they would receive an evaluation of their interview via email.

3.2.2 Phase 2: At home, privacy-invasion phase including email with experimental manipulation

One day after the interview, participants received an email containing links to a text evaluation and a video of the interview (see Appendix Table 3 for the email). However, the email was addressed to another supposed participant of the same study named "Luca". This way, participants were tricked to believe that they received an email actually intended for another person. In the email, Luca was thanked for their participation and was informed that they will receive the evaluation of their interview via two links contained in this email. The email further informed the recipient that the first link will direct them to a text file that presents an evaluation of the

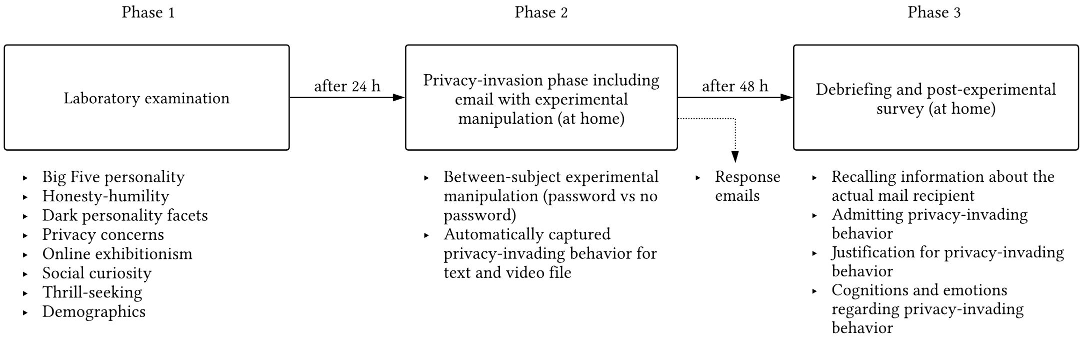
Phase 1
Phase 2
Phase 3
Laboratory examination
after 24 h
Privacy-invasion phase including email with experimental manipulation (at home)
after 48 h
Debriefing and post-experimental survey (at home)
Response emails
Big Five personality
Honesty-humility
Dark personality facets
Privacy concerns
Online exhibitionism
Social curiosity
Thrill-seeking
Demographics
Between-subject experimental manipulation (password vs no password)
Automatically captured privacy-invading behavior for text and video file
Recalling information about the actual mail recipient
Admitting privacy-invading behavior
Justification for privacy-invading behavior
Cognitions and emotions regarding privacy-invading behavior

Figure 1: Flow chart of the study procedure. Items below the boxes indicate the measured variables. See Section 3.2 for further details.

interview and that the second link will direct them to a video file of their interview that has been conducted in phase 1.

At this point, we experimentally manipulated the effort necessary to access the other person's private information. In one group, the email contained information that access to the text and video files is password-protected using the email recipient's first name (thus, the correct password was "Luca"). The links for this group led to a page where participants were asked for the password and only after correctly inputting the password the files could be accessed. In the other group, no password protection was mentioned and the links led directly to a page with the respective files. The web pages containing the text and the video file logged the duration of accessing the information.

At this point, some people wrote us that they received a mail containing evaluation materials from another person. We responded that we will clarify what happened but did not disclose our experiment. Disclosing our experiment would have destroyed our manipulation and participants who wrote us an email might have reacted differently to our final survey (see Phase 3).

3.2.3 Phase 3: At home, debriefing-phase and post-experimental survey

Two days after the first email, participants received an apology and information that due to a technical error several emails had been sent to wrong recipients (see Appendix Table 4 for the content of this email). To uphold the cover story, the email asked participants to respond to another questionnaire that was supposedly aimed towards estimating the extent of this supposed error (details on the questionnaire in phase 3 see section 3.3 and Appendix Table 6). First, participants were asked multiple-choice questions to assess whether they had received an email to make sure that phase 2 worked as intended. Then, participants were asked open-response questions that captured whether participants remembered the name of the person who was the actual recipient of the email, whether and how they realized that they had received a wrong email, and whether they remembered details about the other person. Afterwards, participants responded to a manipulation check for the password condition (i.e., "Were you asked to insert a password at any point?"). Subsequently, participants were asked whether they accessed the other person's private information, thus recording whether participants admitted their potential PIB. Participants were then asked to justify their possible PIB via an open-ended question.

Then, participants were debriefed about the actual objective of the study. Specifically, they were informed that the objective was to examine whether people would access other's private information when given the opportunity to do so and whether they would admit accessing this private information. Furthermore, we told participants that we covertly captured whether they accessed the other person's text and/or video file thus informing them that we knew whether they accessed the files. We emphasized that we never recorded or stored their interview answers and there was no leakage of their private information. Afterwards, participants were asked about the credibility of the cover story of the study. In addition, we asked participants about their cognitions and emotions regarding the private information that they accessed and they were once more given the opportunity to justify their potential PIB the same way as before the debriefing.

3.2.4 Rationale for the procedure

To provide detail on the rationale behind the procedure of the current study, we now present prerequisites for our study and consequences that have manifested in our procedure.

1. Participants needed to be immersed into a realistic situation. If it would have been too obvious that the study was about PIB, people might adapt their behavior in a socially-desirable way. *Consequence:* We used the cover of a "job interview study". These studies are common at the main authors' research institution. We also embedded the questionnaires that were central to our research questions with diversion questionnaires that maintained the "job interview" facade.

2. We needed the option to experimentally manipulate the

effort necessary to access another person's private information. Thus, we needed a situation where we could make it harder to access private information and at the same time not too hard for laypeople. *Consequence:* During phase 2, we manipulated the necessary effort using an easy-to-derive password. Having a password makes it implausible that participants just clicked on a link "by accident". Moreover, since we decided to have the password be the name of the actual recipient of the email, typing in the correct password makes it less plausible that participants believed that the information in the email was actually intended to be for them.

3. We needed to covertly capture participants' actual PIB. Since PIB is socially unaccepted, it is not possible to ask people overtly whether they performed such behavior because we can expect that even under the assurance of anonymity, people may not honestly report their behavior [2]. *Consequence:* During phase 2, we covertly captured participants' behavior with the text and video files.

4. To enable us to examine whether participants would admit PIB, we needed a situation where they were asked to report whether they engaged in PIB. *Consequence:* In phase 3, we gave participants the opportunity to admit their behavior before they were debriefed about the study objectives.

5. In studies including deception, ethics requirements demand to debrief participants about the study objectives, and about where they can get more information about the study. *Consequence:* In phase 3, we debriefed participants, informed them about the study objectives, and provided them with the contact details of the principal investigators. Also, we checked whether people accessed the debriefing in phase 3 and contacted participants who did not complete phase 3 to also debrief them.

3.3 Measurements

Participants responded to all items on a scale from 1 to 5 ("strongly disagree" to "strongly agree"). For all scales we report Cronbach's α as a measure of reliability. Reliability of all scales was acceptable or good, except for psychopathy which was not used for further analyses. If items were not available in the study language, we applied a team approach (following [31, 32]). That is, two researchers independently translated the English items into German, discussed possible disparities and resolved them. See https://osf.io/zcq2e for further information on the used items and materials.

Accessing private information. We automatically captured whether people accessed the text and video file. For both files, we also captured how long participants interacted with these files.

Admitting PIB. In phase 3, participants were asked whether they accessed the other person's private information, thus recording whether participants admitted their potential privacy-violating behavior. The respective questions were introduced by the prompt "If you received an email with a personal evaluation that was not intended for you ..." and then captured the possibilities for privacy-violating behavior: "...did you look at the text evaluation file?", and "... did you watch (parts of) the video recording?"

Big Five personality. The Big Five personality dimensions were assessed with the Big Five Inventory (BFI) by John and Srivastava [33] with 44 items in a German version [34]. This inventory captures the personality dimensions openness to experience (e.g., "I see myself as someone who is original, comes up with new ideas"; Cronbach's α = .85), conscientiousness (e.g., "I see myself as someone who does a thorough job"; Cronbach's α = .82), extraversion (e.g., "I see myself as someone who is talkative"; Cronbach's α = .88), agreeableness (e.g., "I see myself as someone who is considerate and kind to almost everyone"; Cronbach's α = .76) and neuroticism (e.g., "I see myself as someone who gets nervous easily"; Cronbach's α = .85).

Honesty-humility. Honesty-humility was captured using 10 items from the HEXACO Personality Inventory-Revised by Ashton and Lee [35]. A sample item was "I wouldn't use flattery to get a raise or promotion at work, even if I thought it would succeed" (Cronbach's α = .76).

Dark personality facets. Dark personality facets were measured with the German version of the Dirty Dozen by Jonason and Webster [19] by Küfner et al. [36]. This scale captures the Dark Triad with its three dimensions Machiavellianism (e.g., "I tend to manipulate others to get my way"; Cronbach's α = .80)., Narcissism (e.g., "I tend to want others to admire me"; Cronbach's α = .70), and Psychopathy (e.g., "I tend to lack remorse"; Cronbach's α = .39), using 12 items (4 per subscale).

Privacy concerns. Privacy concerns were measured with 6 items by Dinev and Hart [37]. A sample item was "I am concerned that the information I submit on the Internet could be misused" (Cronbach's α = .84).

Online exhibitionism. Online exhibitionism was assessed with the Social Exhibitionism on the Internet scale by Vetter et al. [27]. We used the short version of this scale, which measures online social exhibitionism with 8 items. A sample item was "I like to post details of my private life on the internet" (Cronbach's α = .81). Due to the too explicit reference to sexuality, the item "I like to use communication platforms on the Internet to share my sexual fantasies with people I do not know" was removed.

Social curiosity. Social curiosity was measured with the 10-item version of the Social Curiosity Scale by Renner [14]. A sample item was "When other people are having a conversation, I like to find out what it's about."; Cronbach's α = .74).

Thrill-seeking. Thrill-seeking was captured with the five items of the corresponding dimension from the Five-Dimensional Curiosity Scale by Kashdan et al. [13]. A sample item was "The anxiety of doing something new makes me feel excited and alive" (Cronbach's α = .79).

3.4 Qualitative measures

Recalling information. In phase 3 we assessed via open-ended questions whether participants recalled information about the actual mail recipient. Those started with the prompt "If you received an email with a personal evaluation that was not intended for you..." and were followed by three questions to capture a) the name of the supposed other person ("... do you still know to whom this mail was addressed?"), b) whether and how participants realized the alleged error ("... how did you realize that the email was not intended for you?"), and c) details about the supposed other person ("... what information about the other person did you see?").

Justification. Before and after the debriefing in phase 3, participants were asked to justify their possible privacy violations via the open question "If you received an email with a personal evaluation that was not intended for you and you clicked on the link to a text or video file or watched it, why did you do this?".

Cognitions and emotions. Participants were asked to report on their cognitions and emotions regarding the private information that they accessed with the question "What did you think or feel when you were dealing with another person's private information (the text or video file)?"

Response emails. During the study, participants responded to the emails that we had sent them. Since these emails could contain interesting information that informs about participant reactions and behavior, we qualitatively analyzed these emails.

4 Results

4.1 Sample characteristics

Overall, 95 participants took part in our study. All participants gave their informed consent and were compensated for their participation either with course credit or with 5€. Of these participants, 72 (75.8%) were female, 22 (23.2%) male, and one person stated another gender. Participants were $M = 22.96$ ($SD = 5.99$) years old. All participants were undergraduates at a German university and the majority was enrolled in a psychology course (86, 90.5%).

4.2 (Sub-)Samples used for hypothesis testing and control questions

Our entire sample completed the first two phases of the experiment, resulting in data from 95 participants usable for the analysis of determinants of PIB. In phase 3, 81 participants completed the survey. Accordingly, the subsample for the analyses of the determinants of admitting PIB and our qualitative analyses consisted of data from 81 participants. After the debriefing in phase 3, we asked participants whether they believed the scenario of the study. Overall, most participants agreed that they found the emails and the scenario believable ("agree" was coded with 4, range 1 to 5; $M = 3.81$, $SD = 1.13$).

4.3 Investigating hypotheses and RQs

4.3.1 Data structure and analysis plan

To test our hypotheses and RQs, we collected data on two different measures of PIB for each participant: The access/admission of access of the text file and the access/admission of access of the video file. To account for the data structure with two different measurements of PIB per subject (i.e., nested data) and to test our hypotheses/RQs parsimoniously, we decided to analyze our data using a multilevel logistic regression analysis. For our analyses, we used R 4.4.1 [38] and the lme4 package [39] and followed recommendations from the multi-level analysis literature [40, 41]. More specifically, we opted for a step-by-step approach, starting from the simplest model with no predictors and gradually adding predictors to explain our data. Following best practice [40] we tested each model against the respective previous model and rejected more complex models if they could not explain the data significantly better than more parsimonious models to prevent overparameterization.

For, both, the analysis of determinants of PIB and for the question regarding the admittance of this behavior, we specified three models:

1. The Null-Model, containing only a random intercept for the participants. This models that two data points of the dependent variable belong to one participant, but does not consider any predictors.

2. Model 1 extends the Null-Model by adding a predictor for the experimental condition (no-password vs. password). The corresponding fixed effect of this predictor enabled testing of our two hypotheses regarding PIB and admitting this behavior. In addition, a predictor for the type of private information (text vs. video) was added in this model step because we imagined that this may also affect participant behavior.

3. Model 2 extends Model 1 by adding predictors for the individual characteristics in focus of our RQs.

Model comparisons were carried out using AIC values as measures of model fit (lower values indicate better fit) as well as χ^2-difference tests that compare performance of the models to explain the empirical data.

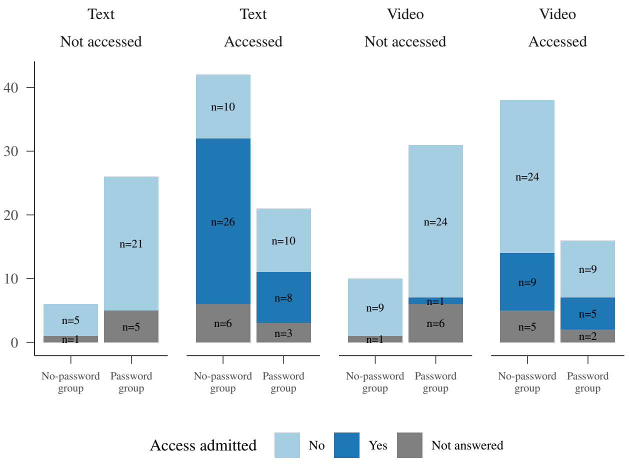

Figure 2: Frequencies of participants per experimental condition who accessed the text and/or video file, of participants who admitted respective behavior, and of participants who did not respond to the respective questions.

4.3.2 Determinants of PIB

Hypothesis 1 stated that participants will show more PIB when accessing the private information requires less effort. Figure 2 provides descriptive information on the number of people who accessed the text and video file, as well as about how many people admitted doing so. In the no-password group, 42 (87.5%) of 48 participants accessed the text file. In the group with password protection, only 21 (44.7%) of 47, accessed the text file. Regarding the video file, in the no-password group, 38 (79.1%) of 48 participants accessed the video file. In the group with password protection, only 16 (34.0%) of 47 participants accessed the video file.

The statistical testing of Hypothesis 1 and the examination of RQ1 followed the multi-level logistic regression approach described in section 4.3.1. Table 1 shows the results of the model comparisons. Model 1 predicted participants' PIB significantly better than the Null-Model ($\chi^2(2) = 35.73$, $p < .001$). Model 2 did not demonstrate a better fit to the data than Model 1 ($\chi^2(12) = 10.06$, $p = .611$). Accordingly, Model 1 was selected as the final model for the dependent variable PIB. Since Model 2 did not explain the empirical data better than Model 1, we found no evidence for any effect of participants' individual characteristics on PIB (see RQ1).

The left side of Table 2 (column: Access) shows the regression coefficients and corresponding significance tests for the final model of PIB. Our results suggest that participants in the password group invaded the other person's privacy significantly less frequently than participants in no-password group (Odds Ratio = 0.03, $p < .001$). This supports Hypothesis 1. We found no effects for the type of information (Odds Ratio = 0.45, $p = .074$).

We further explored our data by examining for how long participants accessed the respective files. The text file was accessed for a mean of $M = 93.13$ ($SD = 137.09$, Median = 35.00) seconds, where 75% of participants accessed the text for longer than 20.5 seconds. Whereas the no-password group accessed the text for a mean of $M = 105.67$ ($SD = 148.84$, Median = 36.50) seconds, the password group accessed the text for a mean of $M = 68.05$ ($SD = 108.87$, Median = 25.00) seconds. The video file was accessed for a mean of $M = 191.82$ ($SD = 244.91$, Median = 60.00) seconds and 75% of the participants who accessed the video did so for longer than 14.50 seconds. Whereas the no-password group accessed the video for a mean of $M = 202.92$ ($SD = 257.69$, Median = 64.00) seconds, the password group accessed the video for a mean of $M = 165.44$ ($SD = 216.99$, Median = 60.00) seconds.

Model	AIC	ICC	R^2	LogLik	χ^2 (df)
Dependent variable: Access ($N = 95$, $Obs. = 190$)					
Null-Model	240.21	.58		-118.11	
Model 1†	208.48	.53	.30	-100.24	**35.73*** (2)
Model 2	222.43	.47	.40	-95.21	10.06 (12)
Dependent variable: Admittance ($N = 60$, $Obs. = 101$)[b]					
Null-Model	143.77	-[a]		-69.88	
Model 1	134.12	.22	.18	-63.06	**13.65*** (2)
Model 2†	126.50	.02	.54	-47.25	**31.62*** (12)

Table 1: Model comparisons for the dependent variables accessing private information (Access) and admitting PIB (Admittance). *Note.* χ^2-scores and df reflect the comparison between the models in the current row vs. the previous row (* denotes a significant improvement). R^2 denotes the marginal R^2 and reflects the proportion of total empirical variance explained by fixed effects only (see [42]) and is thus omitted for the Null-Models.

[a] The Null-Model has a singular fit, meaning that one of the variance components in the model has been estimated as zero. In this case, the variance of the random intercepts for the subjects has been estimated to zero, therefore no ICC can be calculated.

[b] 21 participants were excluded because they did not access neither text nor video file and 14 participants were excluded because they did not answer the survey in phase 3.

† indicates the best model according to model comparison.

4.3.3 Determinants of admitting PIB

Hypothesis 2 proposed that participants will less likely admit PIB when accessing the private information requires more effort. Regarding the text file, 32 participants did not access this file and 9 participants did not respond to the question whether they accessed the text file. Because it was not possible to determine admittance for those participants, they were excluded from the analysis. In the no-password group, 36 participants accessed the text file and 26 of them (72.7%) admitted doing so. In the password group, 18 participants accessed the text file and 8 (44.4%) admitted doing so. Regarding the video file, 42 participants did not access this file and 7 participants did

	Final Model Access				Final Model Admittance			
	Odds Ratio	β	95% *CI*	*p*	Odds Ratio	β	95% *CI*	*p*
Null-Model								
Intercept	20.72	3.03	1.49 – 5.57	**<.001**	0.33	-1.10	-10.67 – 8.47	.821
Model 1								
Type of Information[a]	0.45	-0.79	-1.66 – 0.08	.074	0.10	-2.27	-3.75 – -0.80	**.003**
Experimental Condition[b]	0.03	-3.39	-5.19 – -1.59	**<.001**	0.88	-0.13	-1.42 – 1.17	.849
Model 2								
Openness					2.17	0.77	-0.22 – 1.77	.126
Conscientiousness					0.88	-0.13	-1.11 – 0.86	.804
Extraversion					3.26	1.18	0.10 – 2.26	**.032**
Agreeableness					0.23	-1.46	-3.06 – 0.14	.073
Neuroticism					0.89	-0.12	-1.03 – 0.79	.800
Honesty-humility					1.39	0.33	-0.91 – 1.56	.603
Machiavellianism					0.15	-1.91	-3.27 – -0.55	**.006**
Narcissism					3.75	1.32	-0.04 – 2.69	.058
Privacy concerns					1.01	0.01	-0.84 – 0.87	.976
Thrill-seeking					0.52	-0.65	-0.15 – 0.21	.139
Social curiosity					0.89	-0.12	-1.50 – 1.26	.864
Online exhibitionism					4.69	1.55	0.12 – 2.12	**.034**

Table 2: Regression coefficients of the final models for the dependent variables PIB (Access) and admitting PIB (Admittance).
Note. Significant *p*-values ($\alpha < .05$) are printed bold. [a]Reference category = text. [b]Reference category = no password.

not respond to the question whether they accessed the video file. Because it was not possible to determine admittance for those participants, they were excluded from the analysis. In the no-password group, 33 participants accessed the video and 9 (27.3%) participants admitted doing so. In the password group, 14 participants accessed the video and 5 (35.7%) admitted doing so (see also Figure 2).

Testing of Hypothesis 2 and examining RQ2 followed the multi-level logistic regression approach described in section 4.3.1. Table 1 shows the results of the model comparisons. Model 1 predicted significantly better whether participants admitted their PIB than the Null-Model ($\chi^2(2)$ = 13.65, *p* = .001). Model 2 showed an even better fit to the data than Model 1 ($\chi^2(12)$ = 31.62, *p* = .002). Accordingly, Model 2 was selected as the final model for the further analysis.

The right side of Table 2 (column: Admittance) shows the regression coefficients and corresponding significance tests for the final model of admitting PIB. Participants in the password group were equally likely to admit their PIB like those in the no-password group (Odds Ratio = 0.88, *p* = .849). Accordingly, there was no support for Hypothesis 2. Unexpectedly, we found a significant effects for the type of information (Odds Ratio = 0.10, $p = .003$) in this model. Participants less likely admitted that they had accessed the video (14 out of 47, 29.8%) compared to the text file (34 out of 54, 63.0%). One possible explanation for this effect is that accessing the video file was associated with a stronger feeling of wrongdoing and was thus overall a behavior that people would less likely admit compared to accessing a text file.

RQ2 asked whether individual characteristics affect whether people admit PIB. Based on our model comparisons between Model 1 and Model 2, we conclude that certain individual characteristics affected whether participants admitted PIB. Specifically, higher scores on online exhibitionism (Odds Ratio = 4.69, $p = .034$) and extraversion (Odds Ratio = 3.26, $p = .032$) made it more likely that participants admitted their behavior, whereas higher scores on Machiavellianism (Odds Ratio = 0.15, $p = .006$) made it less likely (see right side of Table 2).

4.3.4 Qualitative results

For further insights regarding why participants behaved and reacted the way they did, we used qualitative analyses to obtain further information from our phase 3 questionnaire and from the emails that participants had sent us. We followed suggestions for reflexive thematic analyses by Braun and Clarke as qualitative analyses [43, 44]. Specifically, in a first step, we coded the text passages in response to the qualitative questions. Second, one of the authors and one research assistant derived superordinate topics from these codings. Third, two independent raters coded all text passages again meaning that they independently assigned text passages to the aforementioned topics. This allowed us to determine reliability of the topics we found in the qualitative analyses. In our case, we calculated interrater reliability (i.e., the agreement between the two raters in assigning the text passages to the superordinate categories). Precisely, we used Cohen's κ which is calculated using the percentage of matches out of the total number of codings, plus adjusting for the probability of random matches. All of our qualitative analyses showed good to excellent reliability with Cohen's κ values between .65 and .91. The procedure was the same for all qualitative questions from the phase 3 questionnaire as well as for the email texts. Of the 95 participants, 14 participants did not respond to the post-experimental survey so it was not possible to include them in the qualitative analysis, accordingly, the following analyses are based on a sample of 81 participants.

Recalling information about the actual mail recipient. The majority of participants recalled the name of the actual mail recipient (70, 86.4%). Participants were also asked whether they recalled information that made them aware of the fact that the email was not meant for them. Many participants noticed through the salutation in the email that it was not their name (73, 90.1%). Participants also reported that they noticed that the email was not meant for them due to the text file (16, 19.8%), the video file (19, 23.5%), or the password (8, 9.9%; i.e. they typed in their own first name to access the files instead of the name "Luca" which was the name of the correct recipient). In summary, these results indicated that the majority of participants realized that the information they received was meant for another person. Importantly, 90.1% of participants already realized through the salutation in the email that this email was not meant for them.

Justification for PIB. Many participants justified accessing the text and/or video by stating that they wanted to check whether the email salutation was just addressed to the wrong person but the files were the correct ones (46, 56.8%). Others remarked that they were interested in the analysis (13, 16.0%) or that they did not notice the wrong salutation (8, 9.8%). A minority stated that they believed that we send a wrong information on purpose (2, 2.5%). These findings imply that many participants justified their behavior with "checking behavior" – they supposedly wanted to check whether the provided information was really not meant for their eyes. Fewer participants justified their behavior by reporting that they were interested in the other person's information. After the debriefing, participants' justifications did not change compared to pre-briefing meaning that they did not change their justification after being informed that we had covertly captured their PIB in phase 2.

Cognitions and emotions regarding PIB. Our results revealed that 30 (37.0%) participants reported negative feelings such as guilt, shame, or concern, 17 (21.0%) participants reported no emotional involvement, and 17 (21.0%) reported that they were concerned about their own private information and who might have access to it. Furthermore, 25 (30.9%) participants expressed empathy with the actual recipient and that they felt bad for them that other people can access their information. Other participants were angry about the mistake (7, 8.6%) and some were suspicious whether this was part of the study or not (6, 7.4%). In sum, these results indicate that participants were (mostly negative) emotionally involved when they realized that they had access to another person's private information. Additionally, participants felt empathy for the other person and at the same time were worried about their own private information as access to another person's private information has made concerns about participants' own privacy salient.

Response emails. Of the 95 participants, 76 (80.0%) responded to our email in phase 2. Of those, 75 (99.0%) wrote that there must have been a mistake during the sending of the mail, that it should be sent to another person or that they are not the person who was addressed in the original email. Furthermore, 14 (18.0%) participants reported concern or anger in their email. They insisted that private data should be handled more conscientiously, that authorities should be informed, and that they wanted immediate clarification of the issue. There were 2 (3.0%) participants who personally came to the laboratory where phase 1 was conducted to contact the research assistants who conducted the study. Also, 14 (18.0%) participants expressed privacy concerns (e.g., concerns about what has happened to their own data). Additionally, 13 (17.0%) participants wanted to make us aware of their privacy-respecting behavior in that they reported that they did not look at anything, that they stopped immediately after realizing that it was not their information, or that they deleted the material instantly. Also, 7 (9.0%) participants explicitly mentioned the full name of the supposed other person. Since the full name of this person was only visible after having clicked on at least one of the links, this indicates that they have accessed the private information. Finally, only 2 (3.0%) participants saw through our mock scenario and wrote that they believe that our email was sent as part of the experimental procedure.

5 Discussion

The goal of this paper was to enhance our understanding of sociotechnical environments that may promote or prevent digital PIB by experimentally investigating situational and individual determinants of PIB that have been proposed in prior research [2]. The main findings of our study are that a) a majority of participants showed PIB, b) many participants had negative feelings about access to another person's private information, c) PIB was less likely when it required more effort to access private information, d) participants were less likely to admit PIB if they accessed the video file compared to the text file, and e) individual characteristics (e.g., personality) only had a minor influence on PIB but influenced whether people admitted such behavior. In sum, our findings indicate that it is less a matter of individual characteristics that drove our participants to engage in PIB but they may have been tempted by effortless access to private information. Furthermore, admitting this kind of behavior seems to differ with respect to the kind of information that was invaded and also depends on people's individual characteristics.

5.1 Privacy-invading behavior

Our study supports research that implied that people are tempted to behave in a privacy-invading manner if given the opportunity [2, 11, 45]. In fact, a majority of our participants accessed private information that was clearly addressed to another person. They mostly reported that they had accessed the files to check whether it was really not information that was meant for them. Clearly, there is a high probability that participants clicked on the links to check whether the information is really not supposed to be for their eyes. However, since a large proportion of participants accessed the text and video files for more than just a few seconds, we argue that participants' behavior did not just reflect "checking behavior". We propose that some participants used checking behavior also as a socially desirable response when asked for the reasons for socially unacceptable behavior [46]. In the case of the password group, checking behavior seems even less plausible because they had to enter the original recipient's first name as a password. Still, in the password group, nearly half of participants accessed the text and almost a third of participants the video file. We thus argue that our participants were aware that accessing others' private information is socially unacceptable which is supported by the number of participants who a) responded to our mail to clarify that they had received a mail that was intended for another person, b) reported negative feelings about accessing another person's private information, and c) described concerns about what might have happened to their own data. Yet, many participants still accessed the other person's private information, watched it for more than just a few seconds, and thus showed PIB.

Furthermore, our study supports that situational characteristics can affect PIB: more effort necessary to access others' private information made it less likely that participants showed PIB. Since deriving the password from the information in the email was easy, our study additionally showed that already low required effort decreases the likelihood that people invade others' privacy. This finding is in line with research on technical design to prevent PIB that has shown that even small changes and small increases of possible required effort to observe private information (e.g., not using graphical passwords; increasing the length of passwords; [8, 47]) can prevent privacy invasions.

Beyond the effort necessary to access private information, future research could explore other situational characteristics that may influence PIB. In hindsight, it is possible that having a password did not only affect the necessary effort to access private information but also whether there is an active action necessary, and/or whether available information is considered to be private. First, a password makes it a more active action to access private information compared to just clicking on a link since this may happen nearly automatically [48]. Second, a password might make it salient that information secured with the password is private. In our study, participants in the no-password condition may have been less aware that information accessible through the links is private information worth protecting. In contrast, "protection" and maybe also "privacy" are salient attributes when something is password-encrypted. With our study, we cannot be sure which of these factors were the most influential to reduce PIB but future research can use our analysis as a starting point to investigate the importance of further situational determinants of PIB.

In contrast to situational characteristics, individual characteristics negligibly affected whether participants engaged in PIB. This could mean that there is not much difference between people regarding PIB. Especially in the case of characteristics such as social curiosity where an association with PIB seems straightforward [11, 14] this finding is surprising. One explanation for this finding and a limitation to our study is that participants were predominantly female and mostly students. Although there was was some variance regarding individual differences even in our homogeneous sample, there may be less compared to a more representative sample thus reducing the potential to reveal possible effects of individual differences. Therefore, we do not dismiss that there are individual characteristics that influence PIB but still conclude that situational may be more influential than individual characteristics. In other words, it is less a question of who shows PIB but when and under what circumstances.

5.2 Admitting PIB

We hypothesized that situational characteristics that make PIB less likely would also make it less likely to admit PIB but found no support for this hypothesis. Instead, we unexpectedly found that admitting PIB was less likely for the video than for the text file. Possibly, participants perceived the video as containing more sensitive information than the text file. We do not want to imply that videos are always considered to include more sensitive information than text files; there clearly is textual information that will be considered very sensitive (e.g., bank account information). Nevertheless, our findings support research indicating that people ascribe different value or sensitivity to different information [26] and goes beyond that by showing that people may be less likely to admit that they accessed private information for which they assign particular value. The problem that arises from this is that if people are already less likely to admit wrongdoing in our study, where they did not have to fear any punishment, it is possible that in real-life people will not take responsibility for PIB when accessing sensitive information. On the one hand, this can diminish trust in relationships where admitting wrongdoing could facilitate rebuilding trust [49]. On the other hand, if unintended access to sensitive information makes admittance less likely, this may also decrease the likelihood with which data leaks or data security issues within organizations will be realized [50]. In other words, if people access sensitive, private information they are not supposed to see, this could reveal security issues. However, if people who access this information are not willing to report doing so, such issues will remain undetected. This is a tentative hypothesis that may be worth investigating in future studies. Furthermore, this finding may be useful for information security training in organizations, where it may be necessary to highlight that access to private information can be a sign for security issues and where interventions may need to be implemented to motivate people to report such possible issues.

Whereas individual characteristics did not affect whether participants engaged in PIB, they did influence whether participants admitted their behavior. Admitting PIB was captured by asking participants whether they accessed private information which may have confronted them with their possible wrongdoing. This confrontation may be the point where people with certain individual characteristics may be more (or less) likely to admit PIB. Our findings implied that more extroverted participants more likely admitted PIB. It is possible that for more introverted participants admitting that they have invaded another person's privacy may be unpleasant because they value privacy more than extroverted ones [23, 51]. Consequently, admitting PIB may have been easier for extroverted compared to introverted participants. Furthermore, participants with stronger tendencies regarding online exhibitionism were more likely to admit PIB. Possibly, they were less likely to believe that accessing private information constitutes problematic behavior because they enjoy presenting private information of themselves online [27]. In line with this, admitting PIB may become more likely if people are less aware that such behavior is inadequate. Finally, participants with higher levels of Machiavellianism were less likely to admit PIB. This finding supports previous work finding that people with high levels of Machiavellianism were more likely to misreport their actual behavior [52]. In summary, our findings imply that engaging in PIB is different from admitting to engage in such behavior. Whereas the former was more strongly influenced by the effort necessary to access private information, the latter was influenced by the type of accessed private information and by individual characteristics.

5.3 Design implications

Although our study was aimed towards a better understanding of sociotechnical environments that affect PIB and not towards deriving design implications, we still want to emphasize design implications of our findings. It may sound obvious but to prevent PIB it makes sense to increase the effort necessary to access private information. On the one hand, our study shows that people are tempted to invade others' privacy when there is no effort required. On the other hand, it shows that even flawed security measures (like easy guessable passwords) can reduce PIB. This behavior affects people whose privacy is being invaded and those who invaded other's privacy since a significant proportion of our participants reported negative feelings after showing PIB (see also [2]). To decrease the temptation to engage in behavior that has mostly negative consequences, designers and individuals need to consider ways to increase the effort necessary for possible PIB. For designers, research on shoulder surfing provides examples regarding how to design technology to make accessing private information require more effort (for a review see [8]). For individuals, our recommendation is to consider ways, even seemingly simple ones, to at least increase the effort for others to engage in PIB. The same way that curtains prevent privacy invasions, sending out password-encrypted files reduces the temptation for people who may accidentally have access to these files to engage in PIB – even if the password is easily available.

5.4 Limitations and Future Work

There are at least two limitations that we need to address. First, our sample consisted mostly of female psychology students which decreases the generalizability of our findings. This group of participants may differ in age, gender, and personality variables from a broader population. For instance, employees will have different characteristic and also different motivations when given the opportunity to access sensitive information. Second, although we designed our study to reflect a realistic situation (i.e., accessing private information because an email was mistakenly sent to the wrong recipient; [4]), it is still a specific situation. PIB in other contexts may differ from the situation in our study. For instance, shoulder surfing has the possibility that the observed person will realize the privacy invasion and will show a reaction that immediately affects the observer. Nevertheless, we believe that our conclusions hold for other PIB and that it is important to consider ways to increase the effort necessary to engage in PIB.

6 Conclusion

Research seems to only be beginning to understand the sociotechnical environment in which digital PIB occurs [2, 8]. Our study supports that PIB may be an everyday behavior that many people would show if given the opportunity, and whose likelihood is affected by situational characteristics. Furthermore, admitting this behavior will never be easy but also seems to depend on the kind of information that was accessed and on individual characteristics of the person who has engaged in PIB. Consequently, technical design but also individuals' privacy-securing behavior need to be guided towards preventing situations where people may be tempted to access information that is not meant for them.

A Appendix

Subject: Job interview study evaluation
Hey Luca, Thank you again for your participation in our job interview study. As already announced, we will send a corresponding evaluation to the study participants for whom our analysis tool strongly deflected at one point of the interview. A part of your behavior seems to have been so remarkable for the algorithm that it gave you extreme values. Under the following links we have provided the automatically generated evaluation as well as the recording of your interview. In the evaluation, there are also time stamps for the remarkable parts, which the algorithm threw out. Evaluation: Link Video recording: Link If you have any questions or want personal feedback just contact me again. Best regards, Laura

Table 3: Email from phase 2
Note: Text of the email sent to participants 24 hours after the job interview in the laboratory. The original email was in German and contained links to the research institute and an automatic signature with the contact details of the Lab.

Subject: Error evaluation job interview study
Dear participant, Unfortunately, due to a technical error, there was some confusion in the sending of the personal evaluations. In order to estimate the extent of this error, we kindly ask you to fill out the following questionnaire: Link Answering the questionnaire will take about 5-10 minutes and you will receive 0.25 subject hours as compensation for your efforts. Best regards, Laura

Table 4: Email from phase 3
Note: Text of the email sent to participants 48 hours after the email from phase 2. The original email was in German and contained links to the research institute and an automatic signature with the contact details of the Lab.

Response emails from participants to the emails from phase 2
information / notification about mistake
information / notification about wrong video
own name explicitly mentioned (not just in closing formula)
own name completely absent (not in text nor in closing formula)
privacy concerns
warning / threatening behavior
integrity / privacy-respecting behavior
full name "Luca Schmidt" mentioned
failed cover story

Table 5: Codebook from the reflexive thematic analysis of the response emails
Note: Cohen's $\kappa = .91$

Scale	Item text	Response format
Big-Five-Inventory [34]	I see myself as someone who . .	1 (strongly disagree) to 5 (strongly agree)
Agreeableness	... tends to find fault with others. (r)	
	... is helpful and unselfish with others.	
	... starts quarrels with others. (r)	
	... has a forgiving nature.	
	... is generally trusting.	
	... can be cold and aloof. (r)	
	... is considerate and kind to almost everyone.	
	... is sometimes rude to others. (r)	
	... likes to cooperate with others.	
Conscientiousness	... does a thorough job.	
	... can be somewhat careless. (r)	
	... is a reliable worker.	
	... tends to be disorganised. (r)	
	... tends to be lazy. (r)	
	... perseveres until the task is finished.	
	... does things efficiently.	
	... makes plans and follows through with them.	
	... is easily distracted. (r)	
Extraversion	... is talkative.	
	... is reserved. (r)	
	... is full of energy.	
	... generates a lot of enthusiasm.	
	... tends to be quiet. (r)	
	... has an assertive personality.	
	... is sometimes shy, inhibited. (r)	
	... is outgoing, sociable.	
Neuroticism	... is depressed, blue.	
	... is relaxed, handles stress well. (r)	
	... can be tense.	
	... worries a lot.	
	... is emotionally stable, not easily upset. (r)	
	... can be moody.	
	... remains calm in tense situations. (r)	
	... gets nervous easily.	
Openness	... is original, comes up with new ideas.	
	... is sophisticated in art, music, or literature.	
	... is curious about many different things.	
	... is ingenious, a deep thinker.	
	... has an active imagination.	
	... is inventive.	
	... values artistic, aesthetic experiences.	
	... prefers work that is routine. (r)	
	... likes to reflect, play with ideas.	
	... has few artistic interests. (r)	

Table 6: Items for phase 1 and phase 3
Note: The items for the Social Exhibitionism on the Internet scale (online exhibitionism) are originally in German and were translated to English for the Appendix. (r) = reverse-coded item.

Scale	Item text	Response format
Social curiosity [14]	I'm interested in people. When other people are having a conversation, I like to find out what it's about. I like finding out how others "work." When on the train, I like listening to other people's conversations. I find it fascinating to get to know new people. When people quarrel, I like to know what's going on. When I meet a new person, I am interested in learning more about him/her. Every so often I like to stand at the window and watch what my neighbors are doing. I like to learn about the habits of others. I like to look into other people's lit windows.	1 (strongly disagree) to 5 (strongly agree)
Online exhibitionism [27]	The idea that theoretically millions of people could look at my site on the Internet is appealing to me. I like to post details of my private life on the internet. I enjoy putting intimate details of my private life on the Internet. I don't like the idea that unknown people on the Internet get information about my leisure activities from me. (r) I like to post photos showing me on the internet for everyone to see. I enjoy posting private videos of myself on the web for everyone to see. I struggle with not knowing who is reading the information I provide online. (r)	1 (strongly disagree) to 5 (strongly agree)
Dark personality facets [19, 36]	I tend to manipulate others to get my way. I have used deceit or lied to get my way. I have use flattery to get my way. I tend to exploit others towards my own end. I tend to lack remorse. I tend to not be too concerned with morality or the morality of my actions. I tend to be callous or insensitive. I tend to be cynical. I tend to want others to admire me. I tend to want others to pay attention to me. I tend to seek prestige or status. I tend to expect special favors from others.	1 (strongly disagree) to 5 (strongly agree)
Privacy concerns [37]	I am concerned that the information I submit on the Internet could be misused. When I shop online, I am concerned that the credit card information can be stolen while being transferred on the Internet. I am concerned about submitting information on the Internet, because of what others might do with it. I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee. When I am online, I have the feeling of being watched. When I am online, I have the feeling that all my clicks and actions are being tracked and monitored.	1 (strongly disagree) to 5 (strongly agree)

Table 6: Items for phase 1 and phase 3
Note: The items for the Social Exhibitionism on the Internet scale (online exhibitionism) are originally in German and were translated to English for the Appendix. (r) = reverse-coded item.

Scale	Item text	Response format
Thrill-seeking [13]	The anxiety of doing something new makes me feel excited and alive.	1 (strongly disagree) to 5 (strongly agree)
	Risk-taking is exciting to me.	
	When I have free time, I want to do things that are a little scary.	
	Creating an adventure as I go is much more appealing than a planned adventure.	
	I prefer friends who are excitingly unpredictable.	
Honesty-humility [35]	I wouldn't use flattery to get a raise or promotion at work, even if I thought it would succeed.	1 (strongly disagree) to 5 (strongly agree)
	If I knew that I could never get caught, I would be willing to steal a million dollars. (r)	
	Having a lot of money is not especially important to me.	
	I think that I am entitled to more respect than the average person is. (r)	
	If I want something from someone, I will laugh at that person's worst jokes. (r)	
	I would never accept a bribe, even if it were very large.	
	I would get a lot of pleasure from owning expensive luxury goods. (r)	
	I want people to know that I am an important person of high status. (r)	
	I wouldn't pretend to like someone just to get that person to do favors for me.	
Controll questions	Did you receive an email from us with an evaluation?	1 (yes), 2 (no)
	Please check your spam folder. Did you find an email from us with an evaluation?	
	If you received an evaluation, was it your own?	
Recalling information about actual recipient	If you received an email with a personal evaluation that was not intended for you ...	open
	... do you still know to whom this mail was addressed?	
	... how did you realize that the email was not intended for you?	
	... what information about the other person did you see?	
Admitting privacy-invading behavior	If you received an email with a personal evaluation that was not intended for you ...	1 (yes), 2 (no)
	... did you read the content of the mail?	
	... did you click on the link to the evaluation document?	
	... did you look at the evaluation document?	
	... did you click on the link to the video recording?	
	... did you watch (parts of) the video recording?	
	... was there a password prompt at any point?	
Justification	If you received an email with a personal evaluation that was not intended for you and you clicked on the link to a text or video file or watched it, why did you do this?	open
Credibility	I found it credible that a mistake was made when sending out the evaluations.	1 (strongly disagree) to 5 (strongly agree)
Cognitions and emotions	What did you think or feel when you were dealing with another person's private information? (text or video file)	open
Previous experience	Have you experienced a case of privacy violation before?	1 (yes), 2 (no)
	If you have already experienced a case of privacy violation, briefly describe it.	open

Table 6: Items for phase 1 and phase 3
Note: The items for the Social Exhibitionism on the Internet scale (online exhibitionism) are originally in German and were translated to English for the Appendix. (r) = reverse-coded item.

Recalling information about the actual mail recipient		
Information from person	**Recognition other recipient**	**Name recall**
name	name	Luca
evaluation sheet	text file	
video	video	
image	image	
conspicuity from the algorithm	password	
unclear, which information they saw	evaluation (unspecific)	
gender		
age		

Justification, cognitions and emotions regarding privacy-invading behavior	
Cognitions and emotions	**Justification**
strange	to check whether the files were the correct ones
relief that other person reacted similarly	curiosity
embarrassing	not noticed the wrong salutation
impressed by the computer evaluation	believe wrong information was sent on purpose
curiosity	believe attachment is a dummy evaluation
indifference	
negative feelings *guilt*, *shame*, *concern*, *shocked*, *unpleasant*, *bad feeling*, *uncomfortable*, *queasy feeling*, *bad conscience*	
empathy with Luca *process is unfair*, *empathy with Luca*, *feeling sorry for Luca*, *protect the privacy of the other person*	
concern about own data *threatening*, *concern about own data*	
distrust in the study *thought that it was intentional*, *thought that it is only a cover story*	
disappointment / anger *disappointment*, *furious*, *anger*	

Table 7: Codebook from the reflexive thematic analysis of the qualitative questions from the phase 3 survey
Note: Cohen's κ = .65

References

[1] M. Andrejevic, "The work of watching one another: Lateral surveillance, risk, and governance," *Surveillance & Society*, vol. 2, no. 4, pp. 479–497, 2004. [Online]. Available: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3359

[2] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt, "Understanding shoulder surfing in the wild: Stories from users and observers," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver, Colorado, USA: ACM Press, May 2017, pp. 4254–4265. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3025453.3025636

[3] D. Marques, T. Guerreiro, L. Carriço, I. Beschastnikh, and K. Beznosov, "Vulnerability & blame: Making sense of unauthorized access to smartphones," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 1–13. [Online]. Available: https://doi.org/10.1145/3290605.3300819

[4] E. Lieberman and R. C. Miller, "Facemail: Showing faces of recipients to prevent misdirected email," in *Proceedings of the 3rd symposium on Usable privacy and security*, ser. SOUPS '07. New York, NY, USA: Association for Computing Machinery, Jul. 2007, pp. 122–131. [Online]. Available: https://doi.org/10.1145/1280680.1280696

[5] S. Petronio, "Communication privacy management theory," in *The international encyclopedia of interpersonal communication*, C. R. Berger, M. E. Roloff, S. R. Wilson, J. P. Dillard, J. Caughlin, and D. Solomon, Eds. New York, US: Wiley, 2015, pp. 1–9. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118540190.wbeic132

[6] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly*, vol. 20, no. 2, pp. 167–196, Jun. 1996. [Online]. Available: https://www.jstor.org/stable/249477?origin=crossref

[7] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research*, vol. 15, no. 4, pp. 336–355, Dec. 2004. [Online]. Available: https://pubsonline.informs.org/doi/10.1287/isre.1040.0032

[8] L. Bošnjak and B. Brumen, "Shoulder surfing experiments: A systematic literature review," *Computers & Security*, vol. 99, pp. 1–34, Dec. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820302960

[9] W. Goucher, "Look behind you: the dangers of shoulder surfing," *Computer Fraud & Security*, vol. 2011, no. 11, pp. 17–20, Nov. 2011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372311701166

[10] J. Hruska, "Amazon's ring security camera let employees spy on customers," Jan. 2019. [Online]. Available: https://www.extremetech.com/internet/283665-amazons-ring-security-camera-let-employees-spy-on-customers

[11] J. A. Litman and M. V. Pezzo, "Dimensionality of interpersonal curiosity," *Personality and Individual Differences*, vol. 43, pp. 1448–1459, Oct. 2007.

[12] F.-M. Hartung and B. Renner, "Social curiosity and interpersonal perception: A judge× trait interaction," *Personality and Social Psychology Bulletin*, vol. 37, no. 6, pp. 796–814, 2011.

[13] T. B. Kashdan, M. C. Stiksma, D. J. Disabato, P. E. McKnight, J. Bekier, J. Kaji, and R. Lazarus, "The five-dimensional curiosity scale: Capturing the bandwidth of curiosity and identifying four unique subgroups of curious people," *Journal of Research in Personality*, vol. 73, pp. 130–149, Apr. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0092656617301149

[14] B. Renner, "Curiosity about people: The development of a social curiosity measure in adults," *Journal of Personality Assessment*, vol. 87, no. 3, pp. 305–316, Oct. 2006. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1207/s15327752jpa8703_11

[15] R. Parks, H. Xu, C.-H. Chu, and P. B. Lowry, "Examining the intended and unintended consequences of organisational privacy safeguards," *European Journal of Information Systems*, vol. 26, no. 1, pp. 37–65, 2017. [Online]. Available: https://doi.org/10.1057/s41303-016-0001-6

[16] R. Wash, E. Rader, R. Berman, and Z. Wellmer, "Understanding password choices: How frequently entered passwords are re-used across websites," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016, pp. 175–188. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/wash

[17] R. R. McCrae and P. T. Costa Jr., "The five-factor theory of personality." in *Handbook of personality: Theory and research, 3rd ed.* New York, NY, US: The Guilford Press, 2008, pp. 159–181.

[18] K. Lee and M. C. Ashton, "Psychometric properties of the HEXACO personality inventory," *Multivariate Behavioral Research*, vol. 39, no. 2, pp. 329–358, Apr. 2004. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1207/s15327906mbr3902_8

[19] P. K. Jonason and G. D. Webster, "The dirty dozen: A concise measure of the dark triad," *Psychological Assessment*, vol. 22, no. 2, pp. 420–432, Jun. 2010. [Online]. Available: http://doi.apa.org/getdoi.cfm?doi=10.1037/a0019265

[20] T. Halevi, J. Lewis, and N. Memon, "A pilot study of cyber security and privacy related behavior and personality traits," in *Proceedings of the 22nd International Conference on World Wide Web*, ser. WWW '13 Companion. New York, NY, USA: Association for Computing Machinery, May 2013, pp. 737–744. [Online]. Available: https://doi.org/10.1145/2487788.2488034

[21] S. Soldz and G. E. Vaillant, "The Big Five personality traits and the life course: A 45-year longitudinal study," *Journal of Research in Personality*, vol. 33, no. 2, pp. 208–232, Jun. 1999. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0092656699922432

[22] G. Bansal, D. Gefen *et al.*, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems*, vol. 49, no. 2, pp. 138–150, 2010.

[23] C. Liu, R. P. Ang, and M. O. Lwin, "Cognitive, personality, and social factors associated with adolescents' online personal information disclosure," *Journal of adolescence*, vol. 36, no. 4, pp. 629–638, 2013.

[24] D. P. Bhave, L. H. Teo, and R. S. Dalal, "Privacy at work: A review and a research agenda for a contested terrain," *Journal of Management*, vol. 46, no. 1, pp. 127–164, 2020.

[25] S. J. Winter, A. C. Stylianou, and R. A. Giacalone, "Individual differences in the acceptability of unethical information technology practices: The case of machiavellianism and ethical ideology," *Journal of Business Ethics*, vol. 54, no. 3, pp. 273–301, 2004.

[26] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review," *MIS Quarterly*, vol. 35, no. 4, pp. 989–1015, 2011. [Online]. Available: https://www.jstor.org/stable/41409970

[27] M. Vetter, C. Eib, S. Hill-Kloss, P. Wollscheid, and D. Hagemann, "Development and validation of a scale for Social Exhibitionism on the Internet (SEXI)," *Diagnostica (Göttingen)*, vol. 60, no. 3, pp. 153–165, 2014. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-107208

[28] J. P. Simmons, L. D. Nelson, and U. Simonsohn, "False-positive psychology," *Psychological Science*, vol. 22, no. 11, pp. 1359–1366, 2011, pMID: 22006061.

[29] H. G. Hern Jr, H. J. Alter, C. P. Wills, E. R. Snoey, and B. C. Simon, "How prevalent are potentially illegal questions during residency interviews?" *Academic Medicine*, vol. 88, no. 8, pp. 1116–1121, 2013.

[30] J. A. Colquitt, "On the dimensionality of organizational justice: A construct validation of a measure," *Journal of Applied Psychology*, vol. 86, no. 3, pp. 386–400, Jun. 2001. [Online]. Available: http://doi.apa.org/getdoi.cfm?doi=10.1037/0021-9010.86.3.386

[31] J. A. Harkness, B. Edwards, S. E. Hansen, D. R. Miller, and A. Villar, "Designing questionnaires for multipopulation research," in *Survey Methods in Multinational, Multiregional, and Multicultural Contexts*. John Wiley & Sons, Ltd, 2010, pp. 31–57. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470609927.ch3

[32] J. A. Harkness, A. Villar, and B. Edwards, "Translation, adaptation, and design," in *Survey methods in multinational, multiregional, and multicultural contexts*, J. A. Harkness, M. Braun, B. Edwards, T. P. Johnson, L. Lyberg, P. P. Mohler, B.-E. Pennell, and T. W. Smith, Eds. Hoboken, NJ: John Wiley & Sons, Inc., May 2010, pp. 115–140. [Online]. Available: http://doi.wiley.com/10.1002/9780470609927.ch7

[33] O. P. John, S. Srivastava *et al.*, *The Big-Five trait taxonomy: History, measurement, and theoretical perspectives*. University of California Berkeley, 1999, vol. 2.

[34] C. B. Fell and C. J. König, "Cross-cultural differences in applicant faking on personality tests: A 43-nation study," *Applied Psychology*, vol. 65, no. 4, pp. 671–717, 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/apps.12078

[35] M. C. Ashton and K. Lee, "The HEXACO-60: A short measure of the major dimensions of personality," *Journal of Personality Assessment*, vol. 91, no. 4, pp. 340–345, Jul. 2009. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/00223890902935878

[36] A. C. P. Küfner, M. Dufner, and M. D. Back, "Das Dreckige Dutzend und die Niederträchtigen Neun [The dirty dozen and the infamous nine]," *Diagnostica*, vol. 61, no. 2, pp. 76–91, Jan. 2015. [Online]. Available: https://econtent.hogrefe.com/doi/abs/10.1026/0012-1924/a000124

[37] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents - measurement validity and a regression model," *Behaviour & Information Technology*, vol. 23, no. 6, pp. 413–422, Nov. 2004. [Online]. Available: https://doi.org/10.1080/01449290410001715723

[38] R Core Team, *R: A Language and Environment for Statistical Computing*, R Foundation for Statistical Computing, Vienna, Austria, 2021. [Online]. Available: https://www.R-project.org/

[39] D. Bates, M. Mächler, B. Bolker, and S. Walker, "Fitting linear mixed-effects models using lme4," *arXiv preprint arXiv:1406.5823*, 2014.

[40] J. J. Hox, M. Moerbeek, and R. Van de Schoot, *Multilevel analysis: Techniques and applications*. Routledge, 2017.

[41] F. Steele, "Multilevel models for longitudinal data," *Journal of the Royal Statistical Society: series A (statistics in society)*, vol. 171, no. 1, pp. 5–19, 2008.

[42] S. Nakagawa, P. C. D. Johnson, and H. Schielzeth, "The coefficient of determination R^2 and intra-class correlation coefficient from generalized linear mixed-effects models revisited and expanded," *Journal of the Royal Society Interface*, vol. 14, no. 134, p. 20170213, 2017.

[43] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, Jan. 2006. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa

[44] ——, "Reflecting on reflexive thematic analysis," *Qualitative Research in Sport, Exercise and Health*, vol. 11, no. 4, pp. 589–597, Aug. 2019. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/2159676X.2019.1628806

[45] J. R. Frampton and J. Fox, "Monitoring, creeping, or surveillance? A synthesis of online social information seeking concepts," *Review of Communication Research*, vol. 9, pp. 1–42, 2021. [Online]. Available: https://www.rcommunicationr.org/index.php/rcr/article/view/75

[46] A. J. Nederhof, "Methods of coping with social desirability bias: A review," *European Journal of Social Psychology*, vol. 15, no. 3, pp. 263–280, 1985. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ejsp.2420150303

[47] L. Bošnjak and B. Brumen, "Shoulder surfing: From an experimental study to a comparative framework," *International Journal of Human-Computer Studies*, vol. 130, pp. 1–20, Oct. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1071581918305366

[48] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," *IEEE Security & Privacy*, vol. 12, no. 1, pp. 28–38, Jan. 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6585241/

[49] N. Gillespie and G. Dietz, "Trust repair after an organization-level failure," *Academy of Management Review*, vol. 34, no. 1, pp. 127–145, Jan. 2009. [Online]. Available: https://journals.aom.org/doi/10.5465/amr.2009.35713319

[50] P. Mayer, Y. Zou, F. Schaub, and A. J. Aviv, ""Now I'm a bit angry:" Individuals' awareness, perception, and responses to data breaches that affected them," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 393–410. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/mayer

[51] D. L. Stone, "Relationship between introversion/extraversion, values regarding control over information, and perceptions of invasion of privacy," *Perceptual and Motor Skills*, vol. 62, no. 2, pp. 371–376, 1986.

[52] P. R. Murphy, "Attitude, machiavellianism and the rationalization of misreporting," *Accounting, Organizations and Society*, vol. 37, no. 4, pp. 242–259, 2012.