The Myth of the Average User

Improving Privacy and Security Systems through Individualization

Serge Egelman
International Computer Science Institute
Berkeley, CA, USA
egelman@cs.berkeley.edu

Eyal Peer
Bar-Ilan University
Ramat Gan, Israel
eyal.peer@biu.ac.il

ABSTRACT

While individual differences in decision-making have been examined within the social sciences for several decades, they have only recently begun to be applied by computer scientists to examine privacy and security attitudes (and ultimately behaviors). Specifically, several researchers have shown how different online privacy decisions are correlated with the "Big Five" personality traits. In this paper, we show that the five factor model is actually a weak predictor of privacy attitudes, and that other well-studied individual differences in the psychology literature are much stronger predictors. Based on this result, we introduce the new paradigm of *psychographic targeting of privacy and security mitigations*: we believe that the next frontier in privacy and security research will be to tailor mitigations to users' individual differences. We explore the extensive work on choice architecture and "nudges," and discuss the possible ways it could be leveraged to improve security outcomes by personalizing privacy and security mitigations to specific user traits.

CCS Concepts

•Security and privacy → Usability in security and privacy; •Human-centered computing → Human computer interaction (HCI);

1. INTRODUCTION

> *"To understand or predict what a rat will learn to do in a maze, one has to know both the rat and the maze" —Hobart Mowrer [62].*

Over the past two decades, system designers have discovered that many security and privacy controls were not designed with the user in mind; security and privacy problems have proliferated due to poor usability [63]. Noticing this, computer security researchers began performing interdisciplinary research to address human factors, and the field of usable security was born [94]. While usable security research has greatly benefited trustworthy computing as a whole, there continues to be one major shortcoming: systems are being made usable for the "average user," but no one person perfectly fits this definition. Due to a high rate of variance with regard to privacy preferences [50], no one set of privacy settings will accommodate all users. Similarly, high variance among security-related behaviors (e.g., at home vs. at the workplace) is detrimental to an "average user" approach. Subsequently, current systems, when they are designed with the user in mind, are often designed to either satisfy majorities, pluralities, or the most vocal. Likewise, due to varying degrees of risk aversion, technical prowess, or attention to detail—just to name a few possibilities—no single security messaging has been shown to deter all users from engaging in risky behavior. For example, compliance rates for security warnings are usually quite low, despite significant progress being made (e.g., [22, 77, 74, 2, 27]). As a result, security mitigations can only reach local maxima when designed for human beings in general, whereas compliance is likely to improve when designed for an individual.

Simply preventing users from engaging in insecure behaviors often has negative consequences. For instance, if a particular web browser blocks a user from visiting a malicious website, and the user does not understand or believe the message, she might use a different web browser that does not prevent her from accessing that website. As a result, there are many security mitigations that require some amount of interaction with the user in order to convince her that it is truly acting in her best interests. Messaging is therefore needed to make users *want* to engage in secure behaviors.

Given the limited amount of screen real estate that software designers have at their disposal for conveying security messages, it is simply infeasible to include multiple messages in the hope that some subset of these messages will resonate with most users. Similarly, if too much text is present in the messaging—due to the inclusion of multiple messages to appeal to multiple user types—few users are likely to read any of it. For example, Beautement *et al.* showed that users are likely to ignore policies that are perceived to be overly onerous [8]. Thus, the problem is in deciding which message to present to which user: each user should encounter a limited amount of messaging, in order to limit the cognitive burden imposed upon them, but that messaging should be chosen to maximize compliance for the given user.

Psychology researchers have studied how individual differences impact decision-making [4]; literature has shown how particular behaviors are correlated with latent constructs (e.g., attitudes towards risk), and that various scales can

NSPW '15, September 08 - 11, 2015, Twente, Netherlands

ISBN 978-1-4503-3754-0/15/09…$15.00

DOI: http://dx.doi.org/10.1145/2841113.2841115

be used to measure those constructs. If some of these constructs are also predictive of privacy preferences, then measurements of those latent constructs (e.g., using scales or observations of related behaviors) can be used to infer an individual's privacy preferences without directly asking her. Similarly, if other constructs are correlated with security decision-making, then measurements of those constructs can be used to tailor security messaging to result in better security outcomes (e.g., warning messages that appear more salient, and are therefore more likely to be obeyed [12]).

The goal of studying individual differences in decision-making is to deepen the understanding of a certain decision-making phenomena and explore whether a certain effect is more pronounced for individuals who exhibit a high or low degree in one or more individual trait measures. For example, several studies have shown that individuals with low numeracy are less likely to understand health risks that are presented to them, and that they are more susceptible to effects of mood and how the information is presented, framed or ordered [68]. Some preliminary evidence also exists for how individual differences predict privacy attitudes: for instance, Pedersen showed that individuals showing low self-esteem are more likely to seek solitude [65]. System designers may be able to apply this knowledge by creating more restrictive default privacy settings for individuals who are deemed to have lower self-esteem (or vice versa).

In the marketing literature, researchers have long understood and exploited the knowledge that different people react differently to the same stimuli. For instance, Kotler and Keller outline several ways in which marketers target different "segments" of the population by modifying materials to fit target audiences [49]. They discuss four categories of segmentation: geographic, demographic, psychographic, and behavioral. These market segmentation techniques have been in use for over 50 years [73]. While geographic and demographic targeting of advertisements are widely known, and behavioral advertising has recently received a lot of attention in the privacy research community (e.g., [61, 60]), fewer people are likely aware that psychographic factors are also used for segmentation. Psychographic segmentation involves targeting different groups based on their attitudes and beliefs [13]. For instance, Issenberg reported that focus groups of undecided voters in the 2008 election were subjected to psychometric tests to determine whether certain campaign commercials were more effective at persuading "rational" versus "emotional" decision-makers (i.e., voters were segmented based on decision-making styles) [39].

In this paper, we introduce the following new paradigm: *psychographic targeting of privacy and security mitigations*. We believe that users will only be able to approach making optimal privacy and security decisions if the interfaces with which they interact are specifically targeted at their individual traits, through the use of psychographic segmentation. The corollary to this is that by continuing to design for the average user, we will continue to satisfice. Through the implementation of this paradigm, we envision a future in which systems automatically infer the traits of their users, either by directly asking them questions that can be used for segmentation, or unobtrusively through the observation and classification of their behaviors. Once traits are inferred, systems can then dynamically modify human-computer interfaces, so that the interfaces with which humans interact are tailored to their specific traits. For instance, once a system infers that the user is prone to making gut decisions (e.g., based on observations of her interactions with other types of messaging or interfaces), it may decide to dynamically alter a security warning to provoke more of a visceral reaction; whereas if it infers that the user is very calculating, it may dynamically alter the same warning to state a succinct threat model. This type of targeting is needed because neither framing by itself is likely to resonate with all users: a succinct threat model is unlikely to be read by those prone to making gut decisions and an attention-grabbing warning is unlikely to resonate with rational decision-makers if it also does not succinctly explain the threat model. Applying both frames is also unlikely to be successful as the resulting warning message might impose too great a cognitive burden for either user type to pay enough attention to understand the recommended course of action. Thus, these two groups need to be segmented and provided with tailored messaging.

In this paper, we describe an initial set of experiments that we performed to show how certain individual differences are predictive of privacy and security attitudes and behaviors. Contrary to the existing literature on predicting privacy preferences using personality traits, we show that the "Big 5" model is a very weak predictor of privacy preferences, relative to other well-studied individual differences in the psychology literature. Based on this result, we argue that significant research is needed to better understand the individual differences that are most predictive of privacy and security behaviors. Finally, we discuss how these findings could be applied to future systems so that they can tailor their privacy and security mitigations to specific psychographic factors, in order to yield better privacy and security outcomes.

2. RELATED WORK

Individual differences have been previously used to predict, and explain, why different people respond differently to the same stimuli, and work on these questions has been carried out in psychology, marketing, decision-making research, and (to a limited degree) computer security.

2.1 Psychology and Marketing

Ever since Ajzen's Theory of Planned Behavior [1], which posited attitudes, alongside beliefs and subjective norms, as drivers of intentions and behavior, researchers in psychology and other domains have sought to identify attitudinal and trait measures that can predict people's behavior. For example, traits such as emotional intelligence have been shown to be strong predictors of various health-related behaviors [58]. The Big 5 personality model, also known as the "five factor model," is one of the most widely used personality models in the field of psychology [19]. The five dimensions are:

- **Openness to new experiences**: the extent to which someone seeks intellectual stimulation.
- **Conscientiousness**: the extent to which someone is organized or self-disciplined.
- **Extraversion**: the extent to which someone is outgoing and enjoys socializing.
- **Agreeableness**: the extent to which someone is compassionate or empathetic.
- **Emotional Stability**: the extent to which someone is stable versus neurotic, insecure, or nervous.

Review of the correlates of personality dispositions (e.g., the Big 5 personality traits) show they are associated with happiness, physical and psychological health, quality of relationships, occupational choice, satisfaction, and performance, as well as community involvement, criminal activity, and political ideology [69]. Marketers have recognized the value of identifying individual differences among consumers and, as stated earlier, target different "segments" of the population by modifying materials to fit target audiences [49]. Accordingly, some researchers focused on discerning individual differences that could be used to customize marketing and advertising efforts (e.g., [17, 55, 37]). For example, one of the individual differences investigated has been people's Need for Cognition (NFC) [15]. This propensity to seek and process information has been found as a strong mediator in how different people evaluate products [36], respond to different messages and persuasion methods [16], or different advertisements [93]. Relatedly, particularly effective has been the growing use of consumers' personal information for online targeted or behavioral advertising [91]. The privacy implications of behavioral advertising aside (e.g., [61, 90, 81]), individual differences play a substantive role in how different consumers respond to different stimuli.

At their core, the marketing field has a lot in common with the field of computer security. One field employs skilled artisans who craft messages that they believe are very important, but would otherwise receive little attention. The goal of these writers is to use these messages to convince the general public to pay certain costs—monetary or otherwise—in order to receive potential benefits that would otherwise not be obvious to the general public. The other involves mass communication via radio, television, and print.

2.2 Individual Differences in Decision-Making

Studying how individual differences affect people's decisions has flourished in the decision-making literature in the last decade (e.g., [75]), up to the point that a Decision Making Individual Differences Inventory[1] was assembled by various researchers. This online repository contains an extensive array of individual differences measures that relate to decision style or decision approach, measures of risk attitudes and behaviors, cognitive abilities, motivational measures, personality traits, and more.[2]

Researchers who study individual differences in decision-making seek to explore whether a certain effect, which was found to be relevant to many people in general, is, in fact, more or less pronounced for certain individuals who exhibit a high or low degree in a certain trait measure. For example, research has shown how framing the same decision in positive versus negative manners affects judgments and choices [79]. A "95% fat free" yogurt is, usually, judged as having higher quality, and chosen more often, than a "5% fat" yogurt [53]. While this has been shown to be true on average, subsequent studies have shown that, in fact, people who scored high on the "conscientiousness" measure (one of the Big 5 personality traits) were less likely to be influenced by this subtle framing, whereas those high in "agreeableness" were more likely to exhibit the effect [52]. Similarly, such framing effects have been shown to occur mostly amongst participants with high NFC [72].

[1]http://www.sjdm.org/dmidi

[2]For a review of some of the measures, see Appelt *et al.* [4].

Other individual differences measures have also been studied in relation to various situations and decisions. The Cognitive Reflection Task involves three puzzles intended to generate a first intuitive (but wrong) response, which is altered only upon reflection [30]. For instance:

> *"A bat and a ball cost $1.10 in total. The bat costs $1.00 more than the ball. How much does the ball cost?"*

In this case, the correct answer is that the ball costs $0.05, whereas the incorrect "gut" response is $0.10. Individual differences in people's ability to correctly answer these questions has been found to be related to their ability to make better inter-temporal decisions (higher patience) as well as improved consideration of decisions' risks. The General Decision Making Style (GDMS) was designed to assess how individuals approach decisions. It distinguishes between five decision styles: a rational style emphasizes "a thorough search for and logical evaluation of alternatives;" an avoidant style emphasizes postponing and avoiding decisions; a dependent style emphasizes "a search for advice and direction from others;" an intuitive style emphasizes "a reliance on hunches and feelings," and a spontaneous style emphasizes "a sense of immediacy and a desire to get through the decision-making process as soon as possible" [71]. The GDMS has been found to predict various outcomes such as job satisfaction [7] and choice of a college major [31], to name just a couple of examples. Another example is the Domain-Specific Risk-Taking (DoSpeRT) scale [10], which assesses people's propensity to engage in various types of risky behavior in different domains: financial, health/safety, recreational, ethical, and social. This scale has been used to predict various risk-related behaviors in various domains such as investments for retirement [33], alcohol misuse [20], and so forth. These examples illustrate how researchers are more and more engaged in searching for possible mediators and explaining factors that could explicate the mechanisms underlying decision-making phenomena.

2.3 Choice Architecture and Nudges

A sub-field in decision-making research focuses on how parameters of the choice architecture (e.g., framing, order, defaults, etc.) impact people's choices [78]. In a recent review [43], several general "tools" or "nudges" have been identified as effective in promoting safer, healthier, more beneficial, or more moral choices and behaviors. For example, the use of defaults has been shown to promote better investment and pension decisions [56], as well as enrollment in organ donation programs [42].

Although defaults have a considerable impact on people's choices and behavior, Johnson *et al.* suggested that some choice architecture tools could be employed better when certain characteristics of the decision-maker are known [43]. For example, nudging home-owners to reduce energy use by showing how they compare against their neighbors only impacted liberal, and not conservative, households [18]. Some work has indeed followed this direction. For example, a stream of research has focused on identifying the people who are more likely to better comprehend information relating to risks (mainly numerical information relating to health risks) and developed a scale of "numeracy" that measures people's ability to understand and use numerical information [54]. Several studies have shown that individuals with

low numeracy are less likely to understand health risks that are presented to them, and that they are more susceptible to effects of mood and how the information is presented, framed or ordered [68]. Additionally, low numeracy participants seem to take less advantage of numerical information presented to them and thus make suboptimal decisions [66]. The implications of this are that nudges should be tested on various different populations, and once a nudge is revealed to have higher potency among specific populations, a more "targeted" nudging approach could be employed, and is expected to produce better results [43]. We hypothesize that many of these effects also apply to security decision-making (e.g., low numeracy individuals may require different security warnings than high numeracy individuals).

2.4 Security Mitigations and Nudges

Several models have been proposed to help analyze why humans make poor security decisions (e.g., [86, 21]), and researchers have used these models to offer recommendations. For instance, Wu *et al.* showed that passive notifications can be ignored when they are not at users' loci of attention [88]. Egelman *et al.* showed that when less-frequent high-risk warnings appear similar to frequent low-risk security warnings, users start to ignore both [22]. Felt *et al.* showed that smartphone permission warnings are overlooked because they occur too frequently and with poor timing [26]. Egelman and Schechter showed that when a clear threat model is not communicated, users may not believe a risk applies to them [24]. In this vein, usable security research has greatly improved the security interventions to which users are exposed.

At the same time, the improvements that the aforementioned studies yielded, while statistically significant over the *status quo*, still leave much to be desired. For instance, Sunshine *et al.* observed that click-through rates on certificate warnings were reduced from 90% to around 50%, when those warnings were designed following usable security guidelines [77], which suggests that half the population are still likely to become victimized. Reeder *et al.* showed that user-centric access control policy authoring interfaces can increase accuracy from 57% to 84% [67]. However, most of this usable security research has focused on improving security by examining average human behavior and offering guidance for how interfaces used by *all* users could be improved. It is possible (indeed, likely) that the average gains are small because the improvements were only effective on a subset of users. For instance, Felt *et al.* found that by adding a picture of a criminal to the Chrome SSL warning, clickthrough rates significantly decreased from 67.9% to 66.5% [27]. It is possible that the reason for this small average effect was that the new imagery only resonated with a small percentage of the population, and therefore different imagery should be shown to the rest of the population. It is also possible that the change increased compliance for one subset of the population, while decreasing it for another subset. We posit that further gains can be made by differentiating users according to individual traits and offering different intervention designs based on those traits, similarly to how marketers use segmentation to better target advertisements to those most receptive to a particular message.

Moreover, we posit that security and privacy mitigations could be improved in two substantial ways. First, applying lessons from the choice architecture and decision-making literature to design and implement security and privacy mitigations could improve the effectiveness of these interventions. Indeed, some studies have already employed the nudging paradigm to privacy and security (e.g., [85, 6, 84, 83, 3]). While these studies have effectively used nudges, there is still much to be explored and learned; we believe that a more comprehensive, theory-driven approach to the design and implementation of security and privacy nudges could prove more successful.

The second manner by which security and privacy mitigations could be improved, we argue, is by tailoring them according to users' individual differences. This approach has been successfully used in other domains, such as decision-making and marketing (as previously outlined), but has rarely been applied to security or privacy behavior. One recent study suggested individual differences may indeed play a role in certain security choices, such as choosing a wireless network, and presented preliminary results that certain nudges may work better on non-experts than on experts [40]. Both Arianezhad *et al.* and Kelley *et al.* showed that experts examine security cues differently than non-experts [5, 47]. Xu *et al.* showed that privacy behaviors and intentions in organizational settings are mediated by individual concern levels [89]. Finally, both Garg *et al.* and Blythe *et al.* showed that risk communication should be targeted based on demographic factors [32, 12]. Although these studies are relevant to our work, we are not aware of any other research to tailor privacy and security mitigations based on psychographic individual differences.

Most related to this new paradigm, others have examined how privacy preferences may be predicted by using the Big 5 model. For instance, Junglas *et al.* found that agreeableness, conscientiousness, and openness to new experiences all correlate with an individual's concern for using location-based services [46]. Korzaan and Boswell found that agreeableness correlated with "concern for information privacy" [48]. These correlations go beyond self-reported privacy concerns, and can also be observed with regard to behaviors: Gou *et al.* found that aspects of users' public Twitter tweets can be used to infer their Big 5 dimensions [35].

Although researchers have examined the relationship between privacy attitudes and personality, there is little (if any) research about how other individual differences—beyond the Big 5 traits—predict people's privacy attitudes and behaviors. In fact, as we show in the next section, the Big 5 traits are very weak predictors of privacy attitudes, relative to other well-studied individual differences in the psychology literature. Exploring the effect of individual differences on self-disclosure behaviors and preferences may lead to systems that better empower users to act according to their stated privacy preferences. Similarly, since we are unaware of any previous research that has examined how security attitudes and behaviors may correlate with individual differences, we believe that exploring this may lead to higher compliance rates with security messaging.

3. PREDICTING PRIVACY ATTITUDES

We conducted two experiments to correlate psychometrics with privacy attitudes and behaviors. First, we examined whether personality traits—as measured by the Big 5 model—correlate with privacy preferences and privacy-preserving behaviors. Subjects completed the Ten Item Personality Inventory (TIPI) [34], which we found to weakly

correlate with privacy attitudes and privacy-preserving behaviors. Next, we performed a followup experiment to show that constructs relating to risk-taking and decision-making style are much stronger predictors of privacy attitudes. The results of these experiments suggest that psychographic segmentation of privacy and security mitigations is feasible, and that performing this segmentation based on decision-making and risk-taking attitudes is a reasonable starting point.

3.1 Experiment 1: Personality

Our first experiment focused on personality traits (i.e., the Big 5 model [19]) as potential predictors of privacy preferences and behaviors. While we observed that personality traits correlate with preferences and behaviors, consistent with prior research, the overall predictive value is quite low. In this section, we describe our method and result.

3.1.1 Method

In this experiment, participants completed a personality test, as well as several different privacy metrics, which measured both stated preferences (i.e., privacy attitudes) and observed behaviors (i.e., participants' willingness to disclose private information about themselves). The order in which they completed each test was randomized, as was the question ordering within each test.

We measured participants' personality dimensions using the Ten Item Personality Index (TIPI) [34], a 10-question survey instrument featuring two questions per personality dimension.[3] Each question is answered using a Likert scale. We used the five dimensions as independent variables in a regression, which also included demographic factors (i.e., gender, income, and education level) as covariates. Thus, each regression model featured eight independent variables.

Our dependent variables consisted of various privacy attitude and behavior metrics. We examined privacy attitudes using the Privacy Concerns Scale (PCS) [14]. The PCS is a set of 16 Likert-scale questions used to evaluate privacy attitudes on a unidimensional scale with regard to how concerned Internet users are with various scenarios involving misuse of personal information. We also used both the Westin Index [51] and the Internet Users Information Privacy Concerns (IUIPC) scale [57]. The Westin Index measures consumers' general attitudes about privacy using 3 Likert-scale questions that segment the population into three categories: "Fundamentalists," "Pragmatists," and the "Unconcerned." Despite being used for several decades [50], researchers have recently raised questions about its validity [87]. The IUIPC scale features 10 Likert-scale questions evaluated across three dimensions: control over personal information ("Control"), awareness of privacy practices ("Awareness"), and data collection concerns ("Collection").

Finally, we measured privacy behaviors by examining participants' self-disclosure behaviors two different ways. First, we used the 10-item Strahan-Gerbasi version of the Marlowe-Crowne Social Desirability Scale (SDS) [76]. The SDS measures social desirability bias, which is the propensity for people to respond to questions in ways that make them appear more desirable to others. To that end, the scale features 10 true/false statements; half reflect rare socially desirable behaviors (e.g., "I am always a good listener"), whereas the other half reflect common socially undesirable behaviors (e.g., "I sometimes try to get even rather than forgive and forget"). We coded the SDS responses by adding the number of "true" responses to socially undesirable traits with the number of responses of "false" to socially desirable traits. Thus, self-disclosure scores ranged from 0 to 10.

Our second metric for self-disclosure behaviors was an unethical behaviors scale developed by John *et al.* [41]. This scale included 14 items about unethical or immoral behaviors (e.g., "Have you ever stolen anything worth more than $25?") to which participants could respond from 1 (never) to 5 (many times) or skip the item if they wished not to answer it. We followed John *et al.* and coded responses for all items in terms of "Affirmative Admissions Rates" (AARs) [41], which represented the frequency with which participants reported engaging in the unethical or immoral behaviors (i.e., not selecting "never" or skipping the item). We examined the correlation between AARs and SDS scores ($r = 0.243$, $p < 0.0005$) and observed that because they were correlated, the AARs were likely measuring both participants' willingness to admit to unethical behaviors, as well as their actual propensity to engage in them.

To examine whether and how personality traits (measured by the TIPI) predict privacy attitudes and self-disclosure, we ran multiple regression analyses using TIPI, gender, education level and income level as predictors on the following dependent variables: PCS, IUIPC (both overall and the 3 sub-scales), Westin Index, disclosure of socially undesirable traits (SDS) and disclosure of unethical behavior (AARs).

To minimize the likelihood of participants selecting responses to questions at random, we included two attention-check questions. First, the beginning of the survey featured the following instructions and questions:

> *This study requires you to voice your opinion using the scales below. It is important that you take the time to read all instructions and that you read questions carefully before you answer them. Previous research on preferences has found that some people do not take the time to read everything that is displayed in the questionnaire. The questions below serve to test whether you actually take the time to do so. Therefore, if you read this, please answer 'three' on the first question, add three to that number and use the result as the answer on the second question. Thank you for participating and taking the time to read all instructions.*
>
> *I would prefer to live in a large city rather than a small city.* [Strongly disagree (1), (2), (3), (4), (5), (6), Strongly agree (7)]
>
> *I would prefer to live in a city with many cultural opportunities, even if the cost of living was higher.* [Strongly disagree (1), (2), (3), (4), (5), (6), Strongly agree (7)]

We gave participants two opportunities to select "3" and "6," respectively. Upon answering incorrectly a second time, we disqualified them from completing the survey. Additionally, we included an 11th item within the SDS questions: *I do not read the questions in surveys.* We filtered out participants who responded "true" to this question *post hoc.*

[3]The TIPI is one of the most frequently used instruments for measuring the Big 5 traits in the psychology literature, with over 2,000 citations.

We recruited 500 participants from Amazon's Mechanical Turk who were over 18, based in the U.S. (to control for language and culture), and with previous task completion rates above 95%. After filtering out 43 responses (8.6% of 500) based on the second attention-check question (i.e., those who incorrectly answered the first attention-check question were unable to submit the survey), we were left with a sample of 457 valid responses. This of course created a selection bias: we can only report on those who paid attention during the experiment, and therefore leave it as future work to determine how to study those who do not diligently complete online tasks without supervision.

Of our sample, 58.2% were male, and the mean age was 32.91 ($\sigma = 11.19$). Most participants had either completed high school (33%) or held a bachelor's degree (33.3%) or an associate's degree (15.5%). Median income category was \$35K-\$50K and the majority of participants (79%) reported an income lower than \$75K per year.

3.1.2 Results

We performed Principal Component Analysis (PCA) to verify each scale's dimensionality and determined internal reliability using Cronbach's α. PCA with Varimax rotation on the PCS showed two components with eigenvalues greater than 1 that predicted 58.72% of the total variance. However, the second component only added 8.26% to the predicted variance and the reliability of the entire scale was high ($\alpha = .933$) so we treated it as measuring one factor, as prescribed by Buchanan *et al.* [14]. Regarding the IUIPC, PCA showed the three original components predicted 75.18% of the total variance: Control ($\alpha = .792$), Awareness ($\alpha = .776$), and Collection ($\alpha = .908$). We noted that one item was cross-loaded on Collection (.495) and Awareness (.455). Based on the recommendations of Matsunaga [59], we retained the original structure (keeping the item with its intended factor, Awareness). The Westin Index showed adequate reliability ($\alpha = .692$), and we did not assess the internal reliability of the TIPI, as its authors recommend against it [34].[4]

Table 1 summarizes our regression analyses. As can be seen, the Big 5 personality traits had a low predictive ability towards the privacy scales, and the total predicted variance was less than 10% for all dependent variables. Among the personality sub-scales, only Agreeableness predicted the PCS (along with income level); Openness to new experiences was the highest and most stable predictor of IUIPC (overall and all sub-scales), followed by Conscientiousness (which predicted Awareness and Collection, but not Control), Agreeableness (which predicted only Awareness) and Extraversion (which predicted Control). Agreeableness also predicted SDS, followed by Conscientiousness, which also predicted AARs, as did Openness and income level.

For the Westin Index, which classifies individuals into three groups, we performed a multinomial regression analysis with the same predictors. Only education level showed a significant result in predicting classification to the three groups ($\chi^2(14) = 23.95$, $p = .046$), while none of the other variables showed any significant prediction. This corroborates prior research showing that the Westin Index is a poor predictor of privacy preferences or behaviors [87], and therefore we decided to not consider it further.

[4]Reliability is established via test-retest [34], which we decided not to perform due to the high internal reliability of the other scales.

That the Big 5 model is a poor predictor of privacy attitudes and behaviors is not a surprise. Others showed that the Big 5 is unable to predict specific attitudes and behaviors because it only measures coarse concepts [38, 11, 70, 45]. Due to this shortcoming, we see little reason to believe that it would be any better at predicting security attitudes and behaviors (*vis-à-vis* privacy). As a result, we hypothesized that more granular measures from the decision-making literature may prove to be better predictors.

3.2 Experiment 2: Decision-Making

Based on the low predictive value of the Big 5 model on privacy attitudes and behaviors, we performed a second experiment that focused on individual differences in decision-making as potential predictors of privacy attitudes. Overall, we observed that decision-making style and risk-taking attitudes were much better predictors.

3.2.1 Method

We made three changes from our first experiment. First, we did not include the Westin Index, as it performed poorly compared to the other privacy attitudes scales. Second, we also chose not to include behavioral tendency measures (such as the SDS and admissions to unethical behaviors) and focused solely on privacy attitudes scales (i.e., the PCS and IUIPC). Finally, we decided to use decision-making psychometrics as our predictors: Need for Cognition (NFC) [15], the General Decision Making Style (GDMS) scale [71], and the Domain Specific Risk Attitude (DoSpeRT) scale [10].

NFC is a unidimensional scale that measures tendency to engage in "thoughtful endeavors" [15]. The GDMS scale measures decision-making style across five dimensions (rational, avoidant, dependent, intuitive, and spontaneous) [71]. The DoSpeRT measures attitudes towards engaging in risks across five dimensions [10]: financial, health/safety, recreational, ethical, and social. Just as before, the order of all questionnaires was randomized between participants.

We recruited a new cohort of 500 participants from Amazon's Mechanical Turk and required that they had not participated in the previous experiment. Using the same screening requirements as in our previous experiment, we filtered out 4 responses (0.8% of 500). This left us with a sample of 496 participants. Almost half (51%) of our participants were male, and the mean age was 35.33 ($\sigma = 11.6$). Most participants had either completed high school (33%) or held a bachelor's degree (33.5%) or an associate's degree (17.3%). Median income category was \$25K-\$50K and the majority of participants (87%) reported an income lower than \$75K per year. These demographics are very similar to those of our initial experiment.

3.2.2 Results

We first analyzed our data in terms of scale reliability. As before, PCS showed high reliability ($\alpha = .936$). A confirmatory PCA on IUIPC showed the original three factors (this time all items loaded highest on their predicted factor), and the factors showed high reliability ($\alpha = .805$, .829, and .908 for Control, Awareness and Collection, respectively). NFC also showed high reliability ($\alpha = .952$). A confirmatory PCA on GDMS showed that the original five factors all had an eigenvalue larger than 1 and predicted a total of 68.18% of the variance. The factors included the different decision-making styles labeled Rational $\alpha = .787$), Avoidant

	PCS	IUIPC				SDS	AARs
		Overall	Control	Awareness	Collection		
Extraversion	-0.002	-0.085	**-0.108**	-0.066	-0.051	-0.034	0.095
	(0.962)	(0.085)	(0.030)	(0.178)	(0.311)	(0.486)	(0.054)
Agreeableness	**0.129**	0.060	0.029	**0.126**	0.015	**0.218**	-0.063
	(0.011)	(0.233)	(0.562)	(0.011)	(0.770)	(<0.001)	(0.208)
Conscientiousness	0.092	**0.110**	0.083	**0.099**	**0.104**	**0.118**	**-0.190**
	(0.071)	(0.029)	(0.103)	(0.048)	(0.044)	(0.019)	(<0.001)
Emotional Stability	-0.102	**0.110**	-0.107	-0.092	-0.088	0.074	0.061
	(0.067)	(0.046)	(0.054)	(0.093)	(0.115)	(0.179)	(0.266)
Openness	0.074	**0.249**	**0.245**	**0.231**	**0.180**	0.005	**0.109**
	(0.141)	(<0.001)	(<0.001)	(<0.001)	(<0.001)	(0.916)	(0.028)
Income level	**-0.099**	0.059	**0.129**	0.042	-0.006	-0.010	**-0.183**
	(0.033)	(0.197)	(0.005)	(0.360)	(0.896)	(0.821)	(<0.01)
Education level	-0.003	0.050	0.051	0.010	0.062	0.062	-0.042
	(0.952)	(0.279)	(0.270)	(0.831)	(0.187)	(0.177)	(0.360)
Male	-0.091	-0.069	0.008	**-0.095**	-0.091	0.063	-0.024
	(0.064)	(0.155)	(0.863)	(0.050)	(0.065)	(0.190)	(0.617)
F	**3.665**	**5.247**	**4.413**	**6.062**	**5.546**	**6.136**	**6.003**
	(<0.001)	(<0.001)	(<0.001)	(<0.001)	(<0.001)	(<0.001)	(<0.001)
Adjusted R^2	.045	.069	.056	.082	.040	.083	.081

Table 1: Regression analysis with privacy preferences/behaviors as dependent variables and the Big Five personality traits as independent variables, controlling for demographic factors. Numbers in parentheses show the p-value; values in bold are statistically significant at the .05 level.

	PCS		IUIPC							
			Overall		Control		Awareness		Collection	
NFC	-0.038	(0.467)	-0.03	(0.54)	-0.041	(0.419)	-0.005	(0.919)	-0.027	(0.606)
GDMS-Intuitive	**0.175**	(0.001)	**0.149**	(0.002)	0.038	(0.436)	**0.144**	(0.002)	**0.173**	(0.001)
GDMS-Rational	**0.252**	(<0.001)	**0.315**	(<0.001)	**0.301**	(<0.001)	**0.283**	(<0.001)	**0.228**	(<0.001)
GDMS-Avoidant	0.076	(0.142)	0.001	(0.977)	-0.055	(0.272)	-0.038	(0.421)	0.064	(0.219)
GDMS-Dependent	**0.102**	(0.044)	-0.01	(0.831)	-0.06	(0.214)	0.0	(0.993)	0.022	(0.667)
GDMS-Spontaneous	0.000	(1.000)	0.008	(0.895)	-0.055	(0.358)	0.022	(0.699)	0.039	(0.53)
RT-Ethical	0.078	(0.215)	**-0.125**	(0.034)	-0.112	(0.067)	**-0.235**	(<0.001)	-0.02	(0.756)
RT-Health/Safety	**-0.213**	(0.001)	-0.105	(0.090)	-0.064	(0.317)	0.014	(0.816)	**-0.169**	(0.011)
RT-Recreational	**0.116**	(0.040)	-0.003	(0.949)	-0.027	(0.617)	-0.066	(0.199)	0.053	(0.347)
RT-Social	0.072	(0.164)	**0.259**	(<0.001)	**0.230**	(<0.001)	**0.241**	(<0.001)	**0.195**	(<0.001)
RT-Financial	0.032	(0.559)	-0.09	(0.082)	-0.071	(0.184)	**-0.102**	(0.043)	-0.063	(0.259)
Male	**-0.121**	(0.009)	-0.039	(0.363)	-0.024	(0.584)	-0.03	(0.472)	-0.04	(0.381)
Education level	0.005	(0.919)	-0.032	(0.454)	-0.043	(0.337)	-0.003	(0.937)	-0.031	(0.501)
Income level	0.02	(0.665)	-0.054	(0.215)	-0.032	(0.482)	-0.037	(0.387)	-0.06	(0.198)
F	**5.332**	(<0.001)	**11.120**	(<0.001)	**8.123**	(<0.001)	**13.58**	(<0.001)	**5.385**	(<0.001)
Adjusted R^2	.113		.230		.174		.270		.114	

Table 2: Regression analysis with privacy attitudes as dependent variables and decision-making psychometrics as independent variables, controlling for demographic factors. Numbers in parentheses show the p-value; values in bold are statistically significant at the .05 level.

(α = .918), Dependent (α = .809), Intuitive (α = .897), and Spontaneous (α = .863). For the DoSpeRT, a confirmatory PCA showed the original five factors which had an eigenvalue larger than 1 and predicted 53.44% of the total variance: Ethical risk-taking (α = .772); Health/Safety risk-taking (α = .737); Recreational risk-taking (α = .846); Social risk-taking (α = .744); Financial risk-taking (α = .831). Thus, we concluded that our data were reliable, and we proceeded to build our regression models.

Table 2 summarizes the results of multiple regression analyses conducted on all dependent variables (PCS, IUIPC overall and sub-scales) with the NFC, GDMS sub-scales, and DoSpeRT sub-scales as predictors, alongside gender, education and income level as covariates. While NFC did not show a significant correlation with any of the privacy attitudes scales, two GDMS styles significantly predicted privacy attitudes on (almost) all scales: Intuitive and Rational. Given the positive standardized coefficients (between 11% and 27% of variance explained), this suggests that stronger privacy attitudes are the result of rational decision-making, as well as people having "gut feelings" about not wanting to divulge information.

Among the risk-taking measures, social risk-taking significantly predicted almost all of the privacy attitudes scales, and health/safety risk-taking negatively predicted PCS and the collection sub-scale of IUIPC. That is, people who are more likely to challenge social norms are also more likely to question company policies about how personal information is handled. Similarly, those who take fewer health and safety risks are more likely to have stronger concerns about their online privacy.

Comparing the results of our two experiments, we can see that the second model has better fit; averaged across all five dependent variables, the coefficient of determination (R^2) was over three times as large in the second model, relative to the first. Thus, future research to predict privacy attitudes and behaviors should probably focus on decision-making psychometrics, rather than the Big 5 model.

4. DISCUSSION

Continuing our preliminary work, our goal is to design security systems that can take advantage of individual differences to present privacy and security mitigation designs that are optimized for individual users. Exploring the paradigm of "psychographic targeting of privacy and security mitigations" will require answering several questions, including:

1. Which psychographic segments should be targeted (i.e., what are the individual differences around which privacy and security mitigations should be targeted)?
2. How can the segmentation be performed automatically without active user involvement (i.e., designing systems to automatically infer their users' traits)?
3. How can knowledge of a user's individual differences be abused, and how might this be prevented?
4. Which privacy and security mitigations are most likely to benefit from being tailored to individual traits?

In the remainder of this section, we discuss three research goals that will help answer these questions:

1. Researchers need validated tools for measuring users' security attitudes so that future studies can control for users' behavioral intentions.
2. Based on the choice architecture literature that we reviewed in Section 2, researchers need to identify the trait measures that are most predictive of privacy and security behaviors.
3. Researchers need to empirically examine how particular privacy and security mitigations can be tailored based on knowledge of individual differences.

4.1 Goal 1: Measuring Security Attitudes

In order to study the impact of tailoring of security mitigations based on psychographic segmentations, experiments will need to isolate how much of the resulting effects are due to targeting a particular mitigation at a particular trait-measure versus other confounding factors. Whereas demographic traits can be measured and factored into our models (e.g., using demographic surveys or via participant recruitment), participants' security intentions also need to be considered. For instance, without understanding whether or not a participant intended to engage in "good" security behavior, it is impossible to say whether her failure to comply with security messaging was because "it did not speak to her" (i.e., poor targeting) or because she simply does not care about good security practices (i.e., low intentions). Being able to measure the extent to which individuals strive to engage in good security practices will allow researchers to further isolate the effect of targeting different mitigation designs to different psychographic segments. Similarly, having low security intentions may be due to lack of knowledge (of other safer alternatives, for example) or lack of control. Therefore, the ability to measure security behavior intentions will also allow researchers and practitioners to target mitigations to those who are most vulnerable.

While several scales exist for measuring privacy attitudes, we are unaware of any similar scales for measuring security attitudes. Thus, we developed a new scale, which we are calling the Security Behavior Intentions Scale (SeBIS) [23]. We created SeBIS by building a corpus of expert security advice offered to end-users, which we accumulated by examining several sources, ranging from the support websites of various large ISPs (e.g., Verizon [82]) to the U.S. Computer Emergency Readiness Team (US-CERT) [80]. We iteratively modified and removed items, such that the resulting 16 items exhibited desirable psychometric properties: wide applicability, high variance, and high reliability. Each item is a statement about whether the respondent engages in a particular behavior and is scored on a 5-point Likert scale ("never," "rarely," "sometimes," "often," and "always"). Factor analysis yielded 4 dimensions:

- **Device Securement**: Locking screens (e.g., on smartphones or desktops) when not in use.
- **Passwords**: Using strong unique passwords.
- **Proactive Awareness**: Using contextual cues, such as examining the URL bar.
- **Updating**: Keeping software patched and up-to-date.

These four dimensions provide focus areas for improving different types of security mitigations through psychographic segmentation: nudges to motivate users to lock their devices, choose strong and unique passwords, obey security warnings, and apply software updates in a timely manner. Additionally, while the scale shows high variance, consistency over time, discriminant validity, and internal reliability, studies are still needed to better understand how predictive it is of behaviors. While our initial research shows that correlations exist between individual differences in the psychology literature and security intentions, as measured by SeBIS [23], and can be used to model how users might respond to various security mitigations, there are still many unanswered research questions. Future research is needed to demonstrate how these findings can be applied by building systems with security mitigations that adapt to the individual user.

Like most psychometric scales, SeBIS is intended to measure *relative* differences in attitudes towards computer security. As a result, there is no threshold for when someone should necessarily be targeted for additional interventions or training. Instead, it is meant to be used to measure whether one individual is *more* or *less* likely to engage in secure behaviors than another individual. However, research is needed to determine whether or not SeBIS can predict computer security behaviors. If so, it should be used as a covariate in future experiments of security behaviors. Similarly, if we observe no correlation between intentions (as measured by SeBIS) and behaviors, then we can be reasonably assured that our future experiments will not be confounded by users' intentions and routine behavior.

Some of the experiments that we envision may attempt to correlate "device securement" sub-scale scores with participants' usage of screen locking on their desktop/laptop computers, as well as whether they use a PIN/passcode to lock their smartphones or tablets. Other experiments might attempt to correlate "passwords" sub-scale scores with the relative strength of participants' passwords and their password reuse rates across different websites; additional experiments will be targeted at the "proactive awareness" and "updating" sub-scales, as well. In this manner, we can empirically determine the types of security behaviors that SeBIS is able to predict across each of its four dimensions.

We have already begun to examine these correlations using the Security Behavior Observatory (SBO), which is a panel of home computer users who have consented to having their systems instrumented [29]. Using SBO data from

50 households, we found that the SeBIS "updating" subscale significantly correlated with taking responsibility for installing anti-virus (Spearman's $\rho = 0.531$, $p < 0.0005$) or firewall ($\rho = 0.338$, $p < 0.027$) software. None of the other sub-scales were correlated with this behavior (i.e., it exhibited discriminant validity). We plan to validate the other SeBIS dimensions with additional SBO data, and expect others to perform similar experiments in other environments. For instance, one might attempt to correlate "securement" scores with whether users log out of the computer when finished using it, or set it to automatically lock after a certain timeout period; one might attempt to correlate "passwords" scores with the breadth and strength of users' passwords (Florencio and Herley show how this data can be captured in a privacy-preserving manner [28]).

4.2 Goal 2: Identify Psychographic Segments

The brunt of implementing this new security paradigm relies on examining how various privacy and security mitigations can be improved based on knowledge of individual differences. To obtain that, research is needed to develop a corpus of different versions of security mitigations and nudges that could be used in a personalized manner. In parallel, others will need to collate a series of individual differences measures that could be used to tailor security mitigations and nudges to individual users. Finally, a network of relationships will need to be identified to connect each individual difference measure with one (or more) tailored versions of the security mitigation.

From our previous work [23], the five psychometrics that were predictive of SeBIS scores are candidates for inclusion in the preliminary corpus: Need for Cognition (NFC) [15], the Domain Specific Risk Attitude (DoSpeRT) scale [10], the General Decision Making Style (GDMS) scale [71], the Barratt Impulsiveness Scale (BIS) [64], and Consideration for Future Consequences (CFC) [44]. From these scales, several hypotheses present themselves for how different mitigations might be made more effective for various segments of the population. To give a few examples:

- H_1: When risks are framed in terms of economic costs, users measuring low on DoSpeRT-Economic (i.e., less likely to engage in economic risks) will improve their security behaviors at higher rates than users measuring high on DoSpeRT-Economic.
- H_2: When mitigations use social pressure, users measuring high on GDMS-Dependent will improve their security behaviors at higher rates than users measuring low on GDMS-Dependent.
- H_3: When mitigations provide detailed information about why the user should behave a certain way, users measuring low on NFC will improve their security behaviors at lower rates than users measuring high on NFC, because the former are unlikely to read large amounts of text. As a result, when mitigations focus only on attention-grabbing irrelevant cues (e.g., bright colors, flashing warnings, etc.), users measuring low on NFC will improve their security behaviors at higher rates than users measuring high on NFC.
- H_4: When mitigations provide potential future consequences of noncompliance, users measuring low on CFC will improve their security behaviors at higher rates than users measuring high on CFC.

For instance, to evaluate H_2, researchers may create a message during the configuration of a new smartphone that informs participants about the number of their peers who also lock their phones (e.g., using a PIN). Similarly, when encountering web browser phishing warnings during another experiment, researchers may enumerate the number of other people who chose to obey the warnings. Previous research has examined the concept of social navigation for security decisions with varying success (e.g., [9, 25]). We hypothesize that these results have been mixed because the researchers failed to control for dependent decision-making among their participants. Users testing low on NFC (i.e., less curious individuals) may be less likely to update their software when given a verbose list of benefits and details (H_3).

These hypotheses are given as illustrating examples and, as previously mentioned, a considerable amount of effort is needed to generate theory- and evidence-based hypotheses, integrating theories and findings from related studies of the nature and impact of these individual differences from domains such as psychology, marketing, or decision-making. The final outcome of this goal would be a comprehensive and substantiated network of hypotheses connecting individual differences measures with security mitigations and nudges, similar to, but in no way confined to, these examples. Once this network of hypotheses is obtained, they will need to be tested in order to explore the different ways in which security mitigations may be tailored to individual differences. To do this, researchers will likely need to make several software artifacts that can be evaluated on real users, and iterative human subjects experimentation will be required.

4.3 Goal 3: Validating Tailored Mitigations

In order to determine the causal impact of personalized security mitigations, and the mediating role of the individual differences, researchers will need to conduct several experiments and studies directed at firmly testing each of the hypotheses generated by the preceding goal. In each experiment, we expect that several versions of a mitigation will need to be examined, each aimed at a different sub-group defined by the individual difference measure, as well as a control condition that does not include any tailoring, which can be used evaluate the relative effects of each treatment condition across participants (controlling for segmentation).

These experiments will need to test the impact of tailored mitigations for each type of security mitigation. While we theorized about different types of mitigations that may benefit from tailoring based on the 4 SeBIS dimensions, we expect researchers to explore the full spectrum of privacy and security mitigations that may be able to benefit from individualization. We believe that the ultimate goal of research in this area will be in understanding which individual differences should, or should not, be used to tailor security mitigations, how such personalization can be achieved, and the relative effectiveness of each type of personalization on compliance with security mitigations and the subsequent promotion of secure environments.

4.4 Additional Challenges

If we are able to achieve the goals outlined in this section, and personalized security mitigations become widely deployed, additional challenges will remain. Currently, we live in a world where everyone receives the same security messaging and interfaces. If different people receive differ-

ent messaging and interfaces, some may express concern over the fact that their computer's user interface does not look like that of their friends. This may especially pose problems when experts attempt to offer remote assistance to the less savvy (i.e., their descriptions may not actually match what the user sees). Similarly, some users may express concern over *why* they are receiving one particular message over a different one; for example, some may take offense if they infer that their computer has determined that they are impulsive or are incurious (e.g., low NFC). Other users may find that their privacy has been violated because they let someone else use their computer, which revealed the inferences made about the computer's owner.

Of course, these are not new issues; personalization has been applied to other areas of computing over the past two decades. For example, when the Tivo was released, many people expressed concern over the types of programs it recommended for them [92]. "My computer thinks I'm stupid" may replace "my Tivo thinks I'm gay." More broadly, these types of personalized systems will create many future discussions about ethics. For instance, are people being unfairly manipulated? Will they find this creepy? What degree of notice and control should they be given? These questions will need to be addressed as these types of systems become more and more prominent.

Throughout this work, we have focused on relatively stable traits: measures of personality, decision-making style, and risk-taking attitudes. However, we may find that these systems are more effective if they are tailored around unstable traits, such as current emotional state. These questions will need to be examined.

Another future challenge is that the collection of the necessary data is likely to pose privacy and security risks in and of itself. For instance, if computers begin monitoring user behavior to infer traits, this data could be exploited by attackers: the same mechanisms that we suggest be used to make security mitigations more persuasive could also be used to make attacks more effective. This data could also be exploited by other entities that want to learn more about particular users: marketers to create more targeted advertisements, potential employers to screen out undesirable candidates, or even insurance companies to adjust premiums. At a minimum, the data used to make inferences about users needs to be highly protected. This may require differential privacy techniques, decentralization (e.g., a user's data never leaves her device), or aggregating the data in different ways. At the same time, these systems will need to support users with multiple devices and remain consistent when users acquire new devices.

Finally, this is not meant to be a panacea: no matter how much security mitigation interfaces are improved, we are unlikely to ever reach 100% compliance. There will always be users who "fall through the cracks." However, our goal is to optimize, so that the *fewest* possible users make poor security decisions.

5. CONCLUSION

In this paper, we introduce the new paradigm of psychographic segmentation, as it applies to privacy and security mitigations. These principles have long been understood and applied in the marketing domain: advertisement campaigns are made more effective by segmenting the population based on various characteristics, and then providing each segment with different messaging based on its characteristics. We are not aware that these principles have been applied to privacy and security messaging.

Through our initial experiments, we show that privacy attitudes can be predicted by examining several well-studied psychometrics from the psychology literature. While previous research has shown that personality traits are predictive of privacy attitudes (e.g., the Big 5 model), we show that individual differences pertaining to decision-making and risk-taking are much stronger predictors. The purpose of this preliminary work is to illustrate how an individual's privacy and security attitudes can be predicted based on well-studied individual differences in the psychology and decision-making literature. We believe that these findings form the basis for a research agenda into improving privacy and security outcomes by tailoring mitigations around individual differences.

In the future, we envision that systems will be designed to automatically infer "what works" for a given user, in terms of how messaging should be framed, and then dynamically modifying that messaging accordingly.

6. ACKNOWLEDGMENTS

This work was supported by the U.S. National Science Foundation under awards CNS-1343433, CNS-1343451, and CNS-1528070, and by the U.S.-Israel Binational Science Foundation under award 2014626. We would like to thank Alessandro Acquisti, Mary Ellen Zurko, Marian Harbach, and Wolter Pieters for their feedback, as well as Refjohürs Lykkewe.

7. REFERENCES

[1] I. Ajzen. The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2):179–211, 1991.

[2] D. Akhawe and A. P. Felt. Alice in warningland: A large-scale field study of browser warning effectiveness. In *Proceedings of the 22nd USENIX Security Symposium*, 2013.

[3] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. Cranor, and Y. Agarwal. Your location has been shared 5,398 times! a field study on mobile app privacy nudging. Technical Report CMU-ISR-14-116, Carnegie Mellon University, 2014.

[4] K. C. Appelt, K. F. Milch, M. Handgraaf, and E. U. Weber. The decision making individual differences inventory and guidelines for the study of individual differences in judgment and decision-making research. *Judgment and Decision Making*, 6(3):252–262, April 2011.

[5] M. Arianezhad, L. J. Camp, T. Kelley, and D. Stebila. Comparative eye tracking of experts and novices in web single sign-on. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, CODASPY '13, pages 105–116, New York, NY, USA, 2013. ACM.

[6] R. Balebako, P. G. Leon, H. Almuhimedi, P. G. Kelley, J. Mugan, A. Acquisti, L. F. Cranor, and N. Sadeh. Nudging users towards privacy on mobile devices. In *CHI 2011 workshop article*, 2011.

[7] W. K. Balzer. *User's manual for the Job Descriptive Index (JDI; 1997 revision) and the Job in General (JIG) scales*. Bowling Green State University, 1997.

[8] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, NSPW '08, pages 47–58, New York, NY, USA, 2008. ACM.

[9] A. Besmer, J. Watson, and H. R. Lipford. The impact of social navigation on privacy policy configuration. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 7:1–7:10, New York, NY, USA, 2010. ACM.

[10] A.-R. Blais and E. U. Weber. A domain-specific risk-taking (dospert) scale for adult populations. *Judgment and Decision Making*, 1(1):33–47, 2006.

[11] J. Block. A contrarian view of the five-factor approach to personality description. *Psychological bulletin*, 117(2):187, 1995.

[12] J. Blythe, J. Camp, and V. Garg. Targeted risk communication for computer security. In *Proceedings of the 16th International Conference on Intelligent User Interfaces*, IUI '11, pages 295–298, New York, NY, USA, 2011. ACM.

[13] L. Boone and D. Kurtz. *Contemporary Marketing*. Cengage Learning, 2013.

[14] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2):157–165, 2007.

[15] J. T. Cacioppo, R. E. Petty, and C. Feng Kao. The efficient assessment of need for cognition. *Journal of personality assessment*, 48(3):306–307, 1984.

[16] J. T. Cacioppo, R. E. Petty, and K. J. Morris. Effects of need for cognition on message evaluation, recall, and persuasion. *Journal of personality and social psychology*, 45(4):805, 1983.

[17] T. L. Childers, M. J. Houston, and S. E. Heckler. Measurement of individual differences in visual versus verbal information processing. *Journal of Consumer Research*, pages 125–134, 1985.

[18] D. L. Costa and M. E. Kahn. Energy conservation "nudges" and environmentalist ideology: Evidence from a randomized residential electricity field experiment. *Journal of the European Economic Association*, 11(3):680–702, 2013.

[19] P. T. Costa and R. R. McCrae. The revised neo personality inventory (neo-pi-r). *The SAGE handbook of personality theory and assessment*, 2:179–198, 2008.

[20] K. E. Courtney, R. Arellano, E. Barkley-Levenson, A. Gálvan, R. A. Poldrack, J. MacKillop, J. David Jentsch, and L. A. Ray. The relationship between measures of impulsivity and alcohol misuse: an integrative structural equation modeling approach. *Alcoholism: Clinical and Experimental Research*, 36(6):923–931, 2012.

[21] L. F. Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, Berkeley, CA, 2008. USENIX Association.

[22] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceeding of The 26th SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1065–1074, New York, NY, USA, 2008. ACM.

[23] S. Egelman and E. Peer. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '15, New York, NY, USA, 2015. ACM. To appear. Pre-print available at: http://guanotronic.com/~serge/papers/chi15-sebis.pdf.

[24] S. Egelman and S. Schechter. The importance of being earnest [in security warnings]. In *Financial Cryptography and Data Security*, 2013.

[25] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley. Does my password go up to eleven? the impact of password meters on password selection. In *Proceedings of the ACM Computer-Human Interaction Conference*, 2013.

[26] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: user attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, New York, NY, USA, 2012. ACM.

[27] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo. Experimenting at scale with google chrome's ssl warning. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2667–2670, New York, NY, USA, 2014. ACM.

[28] D. Florencio and C. Herley. A large-scale study of web password habits. In *WWW '07: Proceedings of the 16th International Conference on the World Wide Web*, pages 657–666, New York, NY, USA, 2007. ACM Press.

[29] A. Forget, S. Komanduri, A. Acquisti, N. Christin, L. F. Cranor, and R. Telang. Security behavior observatory: Infrastructure for long-term monitoring of client machines. Technical Report CMU-CyLab-14-009, Carnegie Mellon CyLab, 2014.

[30] S. Frederick. Cognitive reflection and decision making. *Journal of Economic perspectives*, pages 25–42, 2005.

[31] K. M. Galotti, E. Ciner, H. E. Altenbaumer, H. J. Geerts, A. Rupp, and J. Woulfe. Decision-making styles in a real-life decision: Choosing a college major. *Personality and Individual Differences*, 41(4):629–639, 2006.

[32] V. Garg, L. J. Camp, K. Connelly, and L. Lorenzen-Huber. Risk communication design: Video vs. text. In *Proceedings of the 12th International Conference on Privacy Enhancing Technologies*, PETS'12, pages 279–298, Berlin, Heidelberg, 2012. Springer-Verlag.

[33] D. G. Goldstein, E. J. Johnson, and W. F. Sharpe. Choosing outcomes versus choosing products: Consumer-focused retirement investment advice. *Journal of Consumer Research*, 35(3):440–456, 2008.

[34] S. D. Gosling, P. J. Rentfrow, and W. B. Swann Jr. A very brief measure of the big-five personality domains. *J. of Research in Personality*, 37(6):504–528, 2003.

[35] L. Gou, M. X. Zhou, and H. Yang. Knowme and shareme: Understanding automatically discovered personality traits from social media and user sharing preferences. In *Proc. of the 32nd Annual ACM Conf.*

on Human Factors in Computing Systems, CHI '14, pages 955–964, New York, NY, USA, 2014. ACM.

[36] C. P. Haugtvedt, R. E. Petty, and J. T. Cacioppo. Need for cognition and advertising: Understanding the role of personality variables in consumer behavior. *Journal of Consumer Psychology*, 1(3):239–260, 1992.

[37] D. L. Hoffman, P. K. Kopalle, and T. P. Novak. The "right" consumers for better concepts: Identifying consumers high in emergent nature to develop new product concepts. *Journal of Marketing Research*, 47(5):854–865, 2010.

[38] L. M. Hough. The 'big five' personality variables–construct confusion: Description versus prediction. *Human Performance*, 5(1-2):139–155, 1992.

[39] S. Issenberg. Born This Way. New York Magazine, April 12 2012. http://nymag.com/news/features/liberals-conservatives-2012-4/.

[40] D. Jeske, L. Coventry, P. Briggs, and A. van Moorsel. Nudging whom how: It proficiency, impulse control and secure behaviour. *Networks*, 49:18, 2014.

[41] L. K. John, A. Acquisti, and G. Loewenstein. Strangers on a plane: context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, 37(5):858–873, 2011.

[42] E. J. Johnson and D. Goldstein. Do defaults save lives? *Science*, 302(5649):1338–1339, 2003.

[43] E. J. Johnson, S. B. Shu, B. G. Dellaert, C. Fox, D. G. Goldstein, G. Häubl, R. P. Larrick, J. W. Payne, E. Peters, D. Schkade, et al. Beyond nudges: Tools of a choice architecture. *Marketing Letters*, 23(2):487–504, 2012.

[44] J. Joireman, M. J. Shaffer, D. Balliet, and A. Strathman. Promotion orientation explains why future-oriented people exercise and eat healthy evidence from the two-factor consideration of future consequences-14 scale. *Personality and Social Psychology Bulletin*, 38(10):1272–1287, 2012.

[45] T. A. Judge and J. E. Bono. Five-factor model of personality and transformational leadership. *Journal of applied psychology*, 85(5):751, 2000.

[46] I. A. Junglas, N. A. Johnson, and C. Spitzmuller. Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4):387–402, print 2008.

[47] T. Kelley, L. J. Camp, S. Lien, and D. Stebila. Self-identified experts lost on the interwebs: The importance of treating all results as learning experiences. In *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results*, LASER '12, pages 47–54, New York, NY, USA, 2012. ACM.

[48] M. L. Korzaan and K. T. Boswell. The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, 48(4):15–24, 2008.

[49] P. Kotler and K. Keller. *Marketing Management*. Pearson Prentice Hall, 2006.

[50] P. Kumaraguru and L. F. Cranor. Privacy indexes: A survey of westin's studies. Technical Report CMU-ISRI-5-138, Carnegie Mellon University, December 2005. http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf.

[51] P. Kumaraguru and L. F. Cranor. Privacy Indexes: A Survey of Westin's Studies. Technical Report CMU-ISRI-5-138, Carnegie Mellon University, December, 2005. http://reports-archive.adm.cs.cmu.edu/anon/isri2005/abstracts/05-138.html.

[52] I. P. Levin, G. J. Gaeth, J. Schreiber, and M. Lauriola. A new look at framing effects: Distribution of effect sizes, individual differences, and independence of types of effects. *Organizational Behavior and Human Decision Processes*, 88(1):411–429, 2002.

[53] I. P. Levin, S. L. Schneider, and G. J. Gaeth. All frames are not created equal: A typology and critical analysis of framing effects. *Organizational behavior and human decision processes*, 76(2):149–188, 1998.

[54] I. M. Lipkus, G. Samsa, and B. K. Rimer. General performance on a numeracy scale among highly educated samples. *Medical Decision Making*, 21(1):37–44, 2001.

[55] D. J. MacInnis, C. Moorman, and B. J. Jaworski. Enhancing and measuring consumers' motivation, opportunity, and ability to process brand information from ads. *The J. of Marketing*, pages 32–53, 1991.

[56] B. C. Madrian and D. F. Shea. The power of suggestion: Inertia in 401 (k) participation and savings behavior. Technical report, National bureau of economic research, 2000.

[57] 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*, 15(4):336–355, December 2004.

[58] A. Martins, N. Ramalho, and E. Morin. A comprehensive meta-analysis of the relationship between emotional intelligence and health. *Personality and individual differences*, 49(6):554–564, 2010.

[59] M. Matsunaga. How to factor-analyze your data right: Do's, don'ts, and how-to's. *International Journal of Psychological Research*, 3(1):97–110, 2010.

[60] A. M. McDonald and L. F. Cranor. Americans' attitudes about internet behavioral advertising practices. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, WPES '10, pages 63–72, New York, NY, USA, 2010. ACM.

[61] A. M. McDonald and L. F. Cranor. Beliefs and behaviors: Internet users' understanding of behavioral advertising. In *38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)*, October 2 2010.

[62] O. H. Mowrer. *Learning theory and behavior*. John Wiley & Sons Inc, 1960.

[63] D. A. Norman. The way i see it: When security gets in the way. *interactions*, 16(6):60–63, Nov. 2009.

[64] J. H. Patton, M. S. Stanford, et al. Factor structure of the barratt impulsiveness scale. *Journal of clinical psychology*, 51(6):768–774, 1995.

[65] D. M. Pedersen. Personality correlates of privacy. *The Journal of Psychology*, 112(1):11–14, 1982.

[66] E. Peters, D. Västfjäll, P. Slovic, C. Mertz, K. Mazzocco, and S. Dickert. Numeracy and decision

making. *Psychological Science*, 17(5):407–413, 2006.

[67] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. Expandable grids for visualizing and authoring computer security policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1473–1482, New York, NY, USA, 2008. ACM.

[68] V. F. Reyna, W. L. Nelson, P. K. Han, and N. F. Dieckmann. How numeracy influences risk comprehension and medical decision making. *Psychological bulletin*, 135(6):943, 2009.

[69] M. K. Rothbart, S. A. Ahadi, and D. E. Evans. Temperament and personality: origins and outcomes. *Journal of personality and social psychology*, 78(1):122, 2000.

[70] R. J. Schneider and L. M. Hough. Personality and industrial/organizational psychology. *International review of industrial and organizational psychology*, 10:75–130, 1995.

[71] S. G. Scott and R. A. Bruce. Decision-making style: The development and assessment of a new measure. *Educational and psychological measurement*, 55(5):818–831, 1995.

[72] S. M. Smith and I. P. Levin. Need for cognition and choice framing effects. *Journal of Behavioral Decision Making*, 9(4):283–290, 1996.

[73] W. R. Smith. Product differentiation and market segmentation as alternative marketing strategies. *Journal of Marketing*, 21(1):pp. 3–8, 1956.

[74] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the challenges in usable security lab studies: Lessons learned from replicating a study on ssl warnings. In *Proceedings of the 2011 Symposium on Usable Privacy and Security (SOUPS '11)*, Jun 2011.

[75] K. E. Stanovich and R. F. West. Individual differences in rational thought. *Journal of experimental psychology: general*, 127(2):161, 1998.

[76] R. Strahan and K. C. Gerbasi. Short, homogeneous versions of the marlowe-crowne social desirability scale. *Journal of clinical psychology*, 1972.

[77] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: an empirical study of ssl warning effectiveness. In *Proceedings of the 18th USENIX Security Symposium*, SSYM'09, pages 399–416, Berkeley, CA, USA, 2009. USENIX Association.

[78] R. Thaler and C. Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press, New Haven and London, 2008.

[79] A. Tversky and D. Kahneman. The framing of decisions and the psychology of choice. *Science*, 211(4481):453–458, January 1981.

[80] United States Computer Emergency Readiness Team. Tips. https://www.us-cert.gov/ncas/tips. Accessed: September 12, 2014.

[81] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 4. ACM, 2012.

[82] Verizon. Security. http://www.verizon.com/Support/Residential/Internet/FiosInternet/General+Support/Security/Security.htm, 2014. Accessed: September 12, 2014.

[83] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh. A field trial of privacy nudges for facebook. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2367–2376. ACM, 2014.

[84] Y. Wang, P. G. Leon, X. Chen, S. Komanduri, G. Norcie, K. Scott, A. Acquisti, L. F. Cranor, and N. Sadeh. The second wave of global privacy protection: From facebook regrets to facebook privacy nudges. *Ohio State Law Journal*, 74:1307–1335, 2013.

[85] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor. Privacy nudges for social media: an exploratory facebook study. In *Proceedings of the 22nd international conference on World Wide Web companion*, pages 763–770. International World Wide Web Conferences Steering Committee, 2013.

[86] M. S. Wogalter. Communication-Human Information Processing (C-HIP) Model. In M. S. Wogalter, editor, *Handbook of Warnings*, pages 51–61. Lawrence Erlbaum Associates, 2006.

[87] A. Woodruff, V. Pihur, S. Consolvo, L. Brandimarte, and A. Acquisti. Would a privacy fundamentalist sell their dna for $1000...if nothing bad happened as a result? the westin categories, behavioral intentions, and consequences. In *Proceedings of the 2014 Symposium on Usable Privacy and Security*, pages 1–18. USENIX Association, 2014.

[88] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 601–610, New York, NY, USA, 2006. ACM.

[89] H. Xu, T. Dinev, J. Smith, and P. Hart. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12):1, 2011.

[90] H. Xu, X. R. Luo, J. M. Carroll, and M. B. Rosson. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1):42–52, 2011.

[91] J. Yan, N. Liu, G. Wang, W. Zhang, Y. Jiang, and Z. Chen. How much can behavioral targeting help online advertising? In *Proceedings of the 18th international conference on World wide web*, pages 261–270. ACM, 2009.

[92] J. Zaslow. If tivo thinks you are gay, here's how to set it straight. *The Wall Street Journal*, 2002. http://www.wsj.com/articles/SB1038261936872356908.

[93] Y. Zhang and R. Buda. Moderating effects of need for cognition on responses to positively versus negatively framed advertising messages. *Journal of Advertising*, 28(2):1–15, 1999.

[94] M. E. Zurko and R. T. Simon. User-centered security. In *NSPW '96: Proceedings of the 1996 Workshop on New Security Paradigms*, pages 27–33, New York, NY, USA, 1996. ACM Press.