Original Research Article

Communication Research
1–31

DOI: 10.1177/00936502231177786
journals.sagepub.com/home/crx


How Can We Increase Privacy Protection Behavior? A Longitudinal Experiment Testing Three Intervention Strategies

Sophie C. Boerman[1], Joanna Strycharz[2], and Edith G. Smit[2]

Abstract

This study investigates which intervention strategies most effectively increase privacy protection behavior. Drawing upon Protection Motivation Theory, we examine the short- and long-term effects of (combinations) of three strategies: (1) increasing awareness of the threat to privacy, (2) training effective privacy protection behavior, and (3) addressing and combating privacy fatigue. We conducted a longitudinal experiment in the Netherlands with three waves (N_{wave1} = 1,000, 2 weeks later N_{wave2} = 799, 2 months later N_{wave3} = 465) and eight between subjects conditions (no strategy and all possible combinations of the strategies). Results show that the training strategy increased self-efficacy and response efficacy, immediately increased all privacy protection behaviors, and positively impacted tracking blocking behavior in the short- and long-term, actual cookie rejection in the short-term (2 weeks later), and deletion behavior in the long-term (2 months later). The threat and fatigue strategies did not have their anticipated effects, but the threat strategy did immediately increase tracking blocking intentions, and the fatigue strategy had a positive, short-term effect on cookie rejection behavior.

Keywords

online privacy, privacy protection behavior, empowerment, longitudinal research, experiment, protection motivation theory

[1]Strategic Communication Group, Wageningen University & Research, Wageningen, The Netherlands
[2]Amsterdam School of Communication Research (ASCoR), University of Amsterdam, The Netherlands

Corresponding Author:
Sophie C. Boerman, Strategic Communication Group, Wageningen University & Research, PO Box 8130, 6700 EW Wageningen, The Netherlands.
Email: sophie.boerman@wur.nl

With everything people do online, they share information—knowingly or unwittingly—with other users, and with commercial, non-commercial, and governmental entities (Acquisti et al., 2015). Digital participation is even believed to be impossible without sharing personal data (Ellison et al., 2007; Kane et al., 2014; Krasnova et al., 2010). We share personal information online to establish and maintain social connections, for our own enjoyment and convenience, to execute commercial transactions, to receive personalized messages and services, and to optimize the performance of websites and apps (e.g., Bansal et al., 2016; Ellison et al., 2007; Gibbs et al., 2011; Krasnova et al., 2010; Robinson, 2017). Next to people sharing information themselves, companies also extract data. The continuous extraction of personal data and our ever-growing dependence upon the digital platforms that enable this are reflected in the notions of "surveillance capitalism" (Zuboff, 2019) and "data capitalism" (West, 2019).

The most important downside and largest issue of the continuous data extraction is the decline of people's informational privacy, which includes people's right to have control over the collection and dissemination of personal information (Baruh et al., 2017; Nissenbaum, 2009). Having informational privacy means being able to determine for yourself when, how, and to what extent information about you is communicated to others (Westin, 1967). Managing and protecting online privacy has become an essential part of everyday life (Büchi et al., 2017). However, research shows that people rarely take action to protect their privacy online, and often do not know how to do this (Boerman et al., 2021), providing evidence for the idea that people often lack informational privacy.

Self-management of online privacy is particularly important as regulations and privacy law (such as the GDPR) mostly delegate the responsibility of privacy protection to users (Degeling et al., 2019; Strycharz et al., 2021). Research has shown that whether people protect their privacy depends on their privacy concerns and attitudes, knowledge, internet and digital skills, experience with privacy violations, education, gender, and age (e.g., Baruh et al., 2017; Büchi et al., 2017; Dienlin & Trepte, 2015; Smit et al., 2014). In addition, privacy protection behavior is negatively influenced by one's level of privacy fatigue (Choi et al., 2018), privacy cynicism (Hoffmann et al., 2016; Lutz et al., 2020), and digital resignation (Draper & Turow, 2019). Thus, to increase one's privacy protection behavior, interventions should boost the factors identified as positive predictors of the behavior and mitigate the negative ones.

To empower internet users and improve their resilience, this study aims to gain insights into which (combination of) intervention strategies aimed at boosting the positive and mitigating the negative factors most effectively increase privacy protection behavior amongst Dutch adults. Building on the Protection Motivation Theory (Rogers, 1975, 1983; Witte, 1992), we propose, develop, and examine three strategies: (1) increasing awareness of the threat to privacy, (2) training effective privacy protection behavior, and (3) addressing and combating privacy fatigue. By doing so, this study contributes to the literature in three ways. First, although prior research has shown that interventions focusing on increasing knowledge and digital literacy can (indirectly) decrease privacy protection amongst adults (Strycharz et al., 2019, 2021)

and children (Desimpelaere et al., 2020), this study is the first to test the effectiveness of intervention strategies that focus on other factors that influence privacy protection, namely the perceived problem severity, efficacy, and privacy fatigue. By doing so, it answers calls to understand how we can combat digital resignation and empower people to manage their privacy (Draper & Turow, 2019). Second, where prior studies only measured immediate effects, we conduct a longitudinal experiment with three waves. This longitudinal approach allows us to test the effectiveness of the strategies immediately after the intervention, on the short-term (2 weeks after the intervention), and on the long-term (2 months later). Such a longitudinal approach is particularly important as it helps to understand whether any intervention effects persist over time and thus truly empower people to protect their privacy in the long term. Third, whereas prior studies focused on very specific privacy behaviors (e.g., rejecting cookies) or a limited set of behaviors, we test the effects on a range of 11 different behaviors that limit both data sharing by users and data collection by companies.

Antecedents of Privacy Protection Behavior

People can protect their online privacy in two ways: by adopting privacy protection measures to limit the data extraction by companies and by limiting the data they share themselves on the internet (Baruh et al., 2017; Büchi et al., 2017). These two behaviors, the use of privacy protection measures and limiting information disclosure, do not seem to be related to each other (Baruh et al., 2017). In this study, we focus on the actual measures that people actively take to protect their privacy by limiting the data extraction by others, such as deliberately rejecting cookies, using opt-out websites and add-ons that limit data tracking, and turning off ad personalization. This excludes limiting information disclosure, such as deliberately not filling out personal information, refraining from posting on social media, or untagging posts or pictures.

Research has shown that people who are more concerned about their privacy, or who have a high desire for privacy, are more inclined to protect their privacy (e.g., Baruh et al., 2017; Büchi et al., 2017; Dienlin & Trepte, 2015). In addition, people who have experience with privacy violations are more likely to take action to protect their privacy (Büchi et al., 2017; Chai et al., 2009). Furthermore, demographic variables such as education, gender, and age seem to be related to privacy protection (e.g., Baruh et al., 2017; Büchi et al., 2017; Dienlin & Trepte, 2015; Smit et al., 2014). More importantly, privacy protection seems to be positively related to individual levels of knowledge, such as privacy literacy (Baruh et al., 2017; Masur, 2020; Park, 2013), knowledge of data collection techniques (Ham, 2017; Ham & Nelson, 2016), and internet skills (Büchi et al., 2017). This is also why the increase of literacy and knowledge is believed to be an effective way to empower people to protect their privacy (Büchi et al., 2017; Masur, 2020; Park, 2013).

Furthermore, there are a few studies that examined the effectiveness of knowledge interventions aiming to increase privacy protection. A study by Desimpelaere et al. (2020) showed that a privacy literacy training enhanced 9 to 13 year-old children's general understanding of data practices and helped them to better protect their privacy

(i.e., limiting information disclosure). However, studies amongst adult samples showed that interventions that increase technical and legal knowledge decreased the perceived severity of and susceptibility to the problem, indirectly making people less inclined to protect their privacy by turning personalization off (Strycharz et al., 2019) or rejecting cookies (Strycharz et al., 2021).

Thus, knowledge interventions may not always have the anticipated empowering effect. One reason for why interventions focusing on knowledge may not be ideal is the so-called "control paradox" (Brandimarte et al., 2013). People with more knowledge are also more confident in dealing with privacy issues, and therefore underestimate the risks, which can result in *more* information disclosure and less privacy protection (Baruh et al., 2017; Brandimarte et al., 2013; Turow & Hennessy, 2007). In line with the control paradox, research showed that people with more knowledge about cookies, online data collection, and data usage appear to be the least concerned about their privacy and are also less inclined to protect their data (Smit et al., 2014). Furthermore, users with more internet and privacy literacy appear to have less privacy concerns (Baruh et al., 2017; Dinev & Hart, 2006). We therefore argue that interventions designed to help people to protect their privacy should focus on other factors than knowledge.

Awareness of the Threat to Privacy

Based upon the Protection Motivation Theory (PMT; Rogers, 1975; Witte, 1992), we first propose an intervention strategy that addresses people's awareness of the threat to their privacy. Considerable studies have applied the PMT to the context of privacy (e.g., Boerman et al., 2021; Dienlin & Metzger, 2016; Ioannou et al., 2021; Strycharz et al., 2019). The PMT stems from health communication research and was developed to understand the factors that drive people's motivation to protect themselves against a health threat. The PMT proposes that the motivation to protect the self from a threat (such as a virus, but in this context, a threat to one's privacy), depends upon the *threat appraisal* and the *coping appraisal*. The threat appraisal consists of the perception of the *severity* of the threat and own *susceptibility* to this threat. The coping appraisal includes perceptions of *self-efficacy* to combat the threat, and the *efficacy* of the possible *response*. When both the threat and coping appraisal are high, the more people are motivated to protect themselves from the threat and adapt their behavior (Witte, 1992).

Drawing upon the PMT, we argue that increasing the perceived threat is an important first step to motivate people to protect themselves against this threat. Prior work that applied the PMT to online privacy has indeed shown that the perceived severity of data collection, usage, and sharing is an important predictor of privacy protection behavior (Boerman et al., 2021; Strycharz et al., 2019, 2021). We therefore propose that one way to increase privacy protection behavior is to address the threat appraisal, by emphasizing both the severity and susceptibility of the threat to people's privacy.

In the design of the threat strategy, we draw upon the Impersonal Impact Hypothesis (Slater et al., 2015; Tyler & Cook, 1984). This hypothesis posits that personal and

societal risk judgments are two different things. So, even if people understand that there is a societal privacy problem, for instance as a result of media coverage of the issue, they may not believe it to be a personal problem (Slater et al., 2015). This notion has clear connections to distinction of perceived severity (i.e., the understanding that there is a severe privacy threat) and perceived susceptibility (i.e., the belief that you can actually experience this threat) in the PMT. Thus, to ensure that people actually understand that the problem is not only severe, but also applies to them personally, we developed an intervention strategy that stresses that privacy threats are personally relevant by directly applying the issues to their own situation. This leads to the following hypotheses:

H1: A strategy addressing the threat of online data collection, usage, and sharing increases the threat appraisal (i.e., perceived severity and susceptibility) (a) immediately after the intervention, in the (b) short- and (c) long-term.
H2: A strategy addressing the threat of online data collection, usage, and sharing increases (a) privacy protection intentions immediately after the intervention, and privacy protection behavior in the (b) short- and (c) long-term.

Training Effective Privacy Protection Behavior

Further building upon the PMT, we also expect strategies focusing on the coping appraisal could be helpful. Following the PMT, efficacy is an important driver of protection motivation. When people do not believe that they can counter a threat, they are unlikely to try to protect themselves against the threat (Rogers, 1975). In the context of privacy, the coping appraisal consists of people's belief in their own ability to protect their privacy on the Internet, that is, self-efficacy, and their belief whether a response effectively prevents threats to privacy, that is, response efficacy (see e.g., Boerman et al., 2021).

Previous research has shown that privacy and internet literacy and skills have a positive influence on privacy protection behavior (Bartsch & Dienlin, 2016; Büchi et al., 2017; Masur, 2020). Looking at the PMT specifically, research found that especially response efficacy influences privacy protection (Boerman et al., 2021). We therefore developed a strategy that focuses especially on increasing people's self-efficacy and response efficacy.

In the design of the training, we focused on two important elements. First, we focus on people's self-esteem and confidence (and thus, self-efficacy). Research has shown that building confidence, esteem, and self-efficacy can remove reluctance and any resistance they may have (Knowles & Linn, 2004). To raise self-efficacy, we develop and test a strategy teaching participants step-by-step how to take specific privacy protection measures (i.e., how to opt-out of personalized advertising, how to only accept necessary cookies, and how to install an add-on that blocks trackers). At the end of each step, participants are praised ("well done"), told what they can now do themselves, and their effort was rewarded with a digital badge. The second important element of the training, emphasizes the effectiveness of the learned measure (to

increase response efficacy) by addressing what this measure actually does (i.e., "You can now see how many trackers on this page are blocked"). To examine the anticipated effects of this strategy, we hypothesize:

H3: Training people to use privacy protection measures increases the coping appraisal (i.e., self-efficacy and response efficacy) (a) immediately after the intervention, in the (b) short- and (c) long-term.
H4: Training people to use privacy protection measures increases (a) privacy protection intentions immediately after the intervention, and privacy protection behavior in the (b) short- and (c) long-term.

Acknowledging and Combating Privacy Fatigue

The inability to protect oneself from a threat is assumed to induce irrational feelings such as helplessness and loss of control (Rogers, 1983). Therefore, we propose that next to the two more cognitive, rational strategies, one could also focus on a more emotional appraisal which is highly relevant in the context of online privacy: *privacy fatigue*. Privacy fatigue or cynicism is described as feelings of uselessness, powerlessness, and mistrust toward the handling of personal data by digital platforms, rendering privacy protection subjectively futile, causing emotional exhaustion and subsequent disengagement and resignation from issues related to online privacy (Choi et al., 2018; Hoffmann et al., 2016; Lutz et al., 2020). This feeling of futility when people do desire to control the information digital entities have about them is also coined "digital resignation" (Draper & Turow, 2019). These feelings of resignation, privacy cynicism, or fatigue are believed to come from the perception that privacy violations are unavoidable (Hargittai & Marwick, 2016).

Research has shown that individual levels of privacy fatigue and privacy cynicism are important predictors of privacy protection behavior (Choi et al., 2018; Hoffmann et al., 2016; Lutz et al., 2020). People that are more fatigued and cynical, feel more powerless, put less effort into making privacy decisions, and thus are less likely to protect their privacy and "do nothing" (Choi et al., 2018; Stanton et al., 2016). Other studies also suggest that people who are resigned to engage in privacy protection often feel that these efforts are futile or unsuccessful (Draper & Turow, 2019; Selwyn & Pangrazio, 2018).

We therefore develop and test a strategy that especially aims at diminishing the feeling of privacy fatigue to increase privacy protection behavior. However, if people have strong feelings of privacy fatigue, they may want to resist a message that tries to change these feelings, for instance by self-assertion (Jacks & Cameron, 2003; Fransen et al., 2015). Self-assertion entails reminding yourself that you are confident about your attitudes (in this case, your privacy fatigue), and that nothing can be done to change these. To overcome this self-assertion, we developed a strategy that focuses on: (1) acknowledging the privacy fatigue, and (2) combatting this fatigue by showing that privacy protection is both simple and effective. By acknowledging the privacy fatigue, we also acknowledge any resistance people may have, which has shown to effectively defuse resistance, making a message more persuasive (Knowles & Linn, 2004).

Privacy fatigue consists of two aspects (Choi et al., 2018): emotional exhaustion (i.e., feeling useless and incapable of doing something about your own privacy), and cynicism (i.e., a feeling that privacy protection is futile). Therefore, the strategy emphasizes for each example that this is both simple, attacking the feeling of being useless and not being able to do something, and effective, attacking the idea that actions are futile. Expecting that this strategy will work, we hypothesize:

H5: A strategy acknowledging and combating privacy fatigue decreases privacy fatigue (a) immediately after the intervention, in the (b) short- and (c) long-term.
H6: A strategy acknowledging and combating privacy fatigue increases (a) privacy protection intentions immediately after the intervention, and privacy protection behavior in the (b) short- and (c) long-term.

Finally, combining one, two, or all three strategies may cause a synergy effect, rendering them even more effective. To examine whether this is true, we also compare all possible combinations of the three strategies.

RQ1: Which (combination of) strategies has/have the largest, positive effect on privacy protection behavior in the short- and long-term?

Method

Design and Sample

To test our strategies, we conducted a longitudinal experiment with a 2 (threat strategy vs. no threat strategy) × 2 (training strategy vs. no training) × 2 (privacy fatigue strategy vs. no privacy fatigue strategy) between subjects design. We manipulated the strategy that people were exposed to and our design led to all possible combinations, resulting in eight experimental conditions (i.e., no strategy; addressing the threat; training effective behavior; acknowledging and combating privacy fatigue; threat and training; threat and fatigue; training and fatigue; and threat, training and fatigue).

The data were collected in November 2020 (wave 1, $N = 1{,}000$), 2 weeks later in December 2020 (wave 2, $N = 799$), and 2 months later in February 2021 (wave 3, $N = 465$) in The Netherlands. All anonymized data are available on OSF: https://osf.io/f4zrs/?view_only=3d9aa627d5a74d73b4a9d692076109d4. The participants were recruited among the members of a national, online research panel consisting of approximately 10,000 active panel members. Based upon a power analysis for repeated measures ANOVA conducted in g*Power, we calculated that to find long-term effects with moderate effect sizes (.20) and statistical power of 0.8, we required 55 participants in each condition in wave 3. In consultation with the panel company, we anticipated a 20% drop-out rate in wave 2 and a subsequent 50% drop-out rate in wave 3. Therefore, we started with a sample of 1,000 participants in wave 1 (min. 116–max. 138 participants per condition). In waves 2 and 3, the panel company invited pools of

Table 1. Sample Descriptions for the Three Waves.

Variable	Wave 1	Wave 2	Wave 3
Age	50.69 (15.70)	50.56 (15.69)	50.78 (15.73)
Gender	47% female	47% female	47% female
Education	16.9% low	16.3% low	14.6% low
	56.7% medium	51.3% medium	48.8% medium
	31% high	32.5% high	36.6% high
Privacy concerns	4.96 (1.34)	4.98 (1.29)	5.03 (1.28)
Attitude toward personalization	3.33 (1.24)	3.67 (1.10)	3.67 (1.09)

participants until we reached the set quota, which resulted in $N = 799$ valid completes in wave 2 (min. 103–max. 110 participants per condition), and $N = 465$ in wave 3 (min. 48–71 max. participants per condition). The sample was representative for the Dutch population with respect to gender, age (18–90 years old), and distribution of educational level. Table 1 shows an overview of the samples in the three waves. In each wave, we excluded participants who did not complete the questionnaire, who did not agree with the informed consent, who used a smart phone to participate in the study (in wave 1), or who failed our attention checks.

Procedure

Participants were invited via the online panel and were redirected to our experiment in Qualtrics. In the first wave, we first screened the participants by asking them to confirm that they were participating on a laptop or computer, preferably using Firefox or Chrome. We decided to only people to participate on a laptop or computer to ensure that the strategies were clearly visible and readable (they were not mobile-friendly). In addition, some of the steps in the training (e.g., installing Ghostery) were specific to laptops and computers. All participants who confirmed to use a laptop or computer were asked to read the study's information and give their informed consent. We asked them to read the information carefully and to follow the instructions. They were also told that they were able to go back and forth if something was unclear. Participants were then randomly assigned to one of eight conditions and were shown either none of the strategies, or an intervention using one strategy or a combination of our strategies. After the intervention, we asked participants about their current privacy protection behavior followed by their intention to perform these behaviors. We then asked an attention check, knowledge, susceptibility, severity (self and other), self-efficacy, response-efficacy, privacy concerns, cost response, attitude toward personalization, privacy fatigue, and digital literacy. We ended the questionnaire with asking participants for their response to the intervention and their demographic information (see all questions and their order in all waves in Table 2).

In the second wave, participants were all directed to a questionnaire that matched the condition of wave 1. These questionnaires started with an informed consent, and

Table 2. Measures in Questionnaires per Wave in Order of Appearance.

Wave 1	Wave 2	Wave 3
	Recall of strategy	
Past privacy behavior	Past privacy behavior	Past privacy behavior
Privacy behavior intention		
Cookie knowledge		
Susceptibility	Susceptibility	Susceptibility
Severity	Severity	Severity
Severity (other)	Severity (other)	Severity (other)
Self-efficacy	Self-efficacy	Self-efficacy
Response efficacy	Response efficacy	Response efficacy
Privacy concerns	Privacy concerns	Privacy concerns
Cost response	Cost response	Cost response
Attitude toward personalization	Attitude toward personalization	Attitude toward personalization
Privacy fatigue	Privacy fatigue	Privacy fatigue
Digital literacy		
Responses to intervention		
Was information new?		
Age	Age	Age
Gender	Gender	Gender
Education	Education	Education

then showed a shortened version of the strategy/strategies. We then asked participants for their current privacy protection behavior, followed by the same measures as wave 1.

The third wave repeated the same informed consent and questions in the same order, but did not include any reminders. All participants were also given the opportunity to download a pdf of the training strategy at the end of wave 3.

Stimulus Materials

We created and pretested several versions of each strategy twice. In Pretest 1, 86 students (M age = 20.69, SD = 2.01, range 18–28; 86% female, 92% finished high school, 8% finished a bachelor's degree) were randomly assigned to one of four preliminary strategies (threat n = 24, training 1 n = 19, training 2 n = 19, fatigue n = 24). We created two versions of the training strategy: version 1 required people to actually take all steps and version 2 only demonstrated how to take the steps. We measured participants' responses to the strategy by means of seven-point semantic differentials (dislike-like, difficult-easy, useless-useful, irrelevant to me-relevant, unclear-clear), perceived severity, self-efficacy, and privacy fatigue (see measures of the final experiment), and asked for feedback to the strategy (open-ended), and whether the information was new to them (0 = *No*, 1 = *Yes*, 2 = *Partly*). Results showed that all strategies

were clear and presented new information, and participants liked and understood them. However, none of the strategies increased severity, $F(3, 82)=0.43$, $p=.735$, or decreased privacy fatigue, $F(3, 82)=0.16$, $p=.922$. Based on these results and the feedback, we adjusted the fatigue strategy so it emphasized that the protecting measures were both effective and simple. We also changed the wording in the threat strategy. Both training strategies led to significantly higher self-efficacy (version 1 $M=4.14$; version 2 $M=4.16$) than the other strategies (threat $M=3.18$; fatigue $M=4.24$), $F(3, 82)=4.70$, $p=.004$. However, as some participants reported problems with actually performing the steps in the same browser as the one used for completing the questionnaire, we decided to further test the training strategy that only demonstrated how to take action. As suggested by participants, we enlarged all images and made sure that participants could download a pdf of the training strategy at the end of the study.

In Pretest 2, we added a control group (no strategy) that served as a baseline, and measured the same variables. We randomly assigned 92 students (M age$=20.30$, $SD=1.50$, range 18–24; 85% female, 88% finished high school or lower, 12% finished a Bachelor's degree) to the revised strategies (threat $n=22$, training $n=22$, fatigue $n=23$) or no strategy ($n=25$). Results showed that the training significantly increased self-efficacy ($M=4.14$) compared to the other strategies (control $M=3.51$; threat $M=2.91$; fatigue $M=3.77$), $F(3, 88)=4.40$, $p=.006$. However, we found no differences between the strategies with respect to perceived severity $F(3, 88)=0.41$, $p=.743$ and privacy fatigue $F(3, 88)=1.10$, $p=.352$. In addition, to test the new fatigue strategy, we specifically explained participants in the fatigue condition the purpose of this strategy and asked whether it succeeded. Most (91%, $n=21$) said yes. We also asked them for their own reasons for privacy fatigue, which we used as input to further develop the strategy. All strategies were liked, and believed to be easy, useful, interesting, relevant, and clear enough (means in pretest 2 consistently >5 on seven-point scales).

All final strategies (see Figure 1 for screen shots) started with explaining the issue: "You've probably heard that companies on the internet collect, use, and share your personal information with other companies in a variety of ways. Are you doing anything to protect your privacy online? You should." (see Panel A in Figure 1). This was all information participants in the no strategy condition got.

The threat strategy continued with: "We know from research that people do not find the collection, usage, and sharing of personal information on the internet as a severe problem. With three examples, we would like to show you that it is." We then explained three risks: (1) sensitive personal profiles using private information to target vulnerable groups and influence you to buy (see Panel B in Figure 1), (2) no control over which companies have what information about you, and (3) personalized pricing.

The training strategy taught participants how to perform three specific behaviors step-by-step: specifically, how to (1) turn off personalization of ads (opt-out) via https://www.youronlinechoices.com (see Panel C in Figure 1), (2) only accept necessary cookies, and (3) install Ghostery to block trackers.

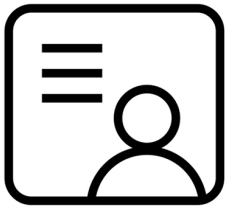
The fatigue strategy first acknowledged people's privacy fatigue ("We know that you are probably tired of privacy issues and do not want to worry about your privacy

A

Je hebt vast wel eens gehoord dat bedrijven op het internet jouw persoonlijke gegevens op allerlei manieren verzamelen, gebruiken, en delen met andere bedrijven.

Doe jij iets om jouw privacy online te beschermen? Dat zou je wel moeten doen.

B



Voorbeeld 1: Gevoelige persoonlijke profielen

Bedrijven op het internet verzamelen openbare gegevens via andere bedrijven (zoals internetwinkels en apps), de overheid, en sociale media.

Ze verdienen er geld mee door de gegevens door te verkopen.

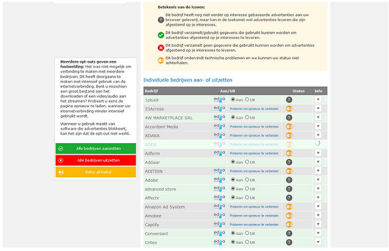
Dankzij deze gegevens kunnen bedrijven **zeer gedetailleerde profielen** samenstellen over mensen.

4

C

Stap 3: Maak een keuze

- Je kunt op deze website zelf bepalen welke bedrijven dit wel of niet mogen doen door te klikken op aan of uit
- Je kunt ook in 1 keer klikken op *Alle bedrijven uitzetten*



16

(continued)

Figure 1. (continued)

Figure 1. Example screenshots of strategies.
Note. Panel A: Introductory text for all strategies, and only information provided in no strategy condition. (Translation: You've probably heard that companies on the internet collect, use, and share your personal information with other companies in a variety of ways. Are you doing anything to protect your privacy online? You should.)
Panel B: Threat strategy explaining that sensitive, personal profiles are created based on personal information. (Translation: Example 1: sensitive, personal profiles. Companies on the internet collect public data from other companies (such as internet shops and apps), the government, and social media. They make money by selling the data. These data allow companies to build very detailed profiles about people.)
Panel C: Training strategy showing step-by-step how to opt-out on https://www.youronlinechoices.com. (Translation: Step 3: make a choice. On this website you can decide for yourself which companies are allowed to do this or not by clicking on or off. You can also click on *Deactivate all companies* in 1 go.)
Panel D: Fatigue strategy emphasizing how only accepting necessary cookies is simple and effective. (Translation: Example 2: take control over cookies. When you visit a website, you are often asked to accept cookies before you can continue. We understand that you often just click *Accept.*
SIMPLE: With a few extra clicks you can also only accept necessary cookies, instead of all cookies.
EFFECTIVE: In this way, no additional information about for example your social media and online behavior is collected and passed on to advertisers.)

online. You may even doubt whether this is necessary or whether it helps.") followed by emphasizing how simple and effective three examples of privacy protection behaviors (identical to the training strategy) are (e.g., "Simple: installing of Ghostery only takes a minute. Effective: Ghostery shows how many and which companies collect your information and can block this automatically. Your information is no longer collected."; see Panel D in Figure 1 for another example).

Measures

Table 2 provides an overview of all measures in the questionnaires of each wave. Tables 3 to 7 present the descriptive statistics of all relevant measures in the three waves.

Table 3. Means and Standard Deviations of Privacy Protection Intention Scores Across the Eight Conditions at Wave 1.

Strategy	Tracking blocking intention	Cookies rejection intention	Deletion intention
Threat	3.33 (1.38)	3.96 (1.36)	3.92 (1.20)
Training	3.99 (1.65)	4.30 (1.44)	4.31 (1.35)
Fatigue	2.86 (1.56)	3.55 (1.51)	4.13 (1.35)
Threat × Training	4.06 (1.71)	4.10 (1.40)	4.06 (1.27)
Threat × Fatigue	3.76 (1.69)	4.10 (1.31)	3.04 (1.44)
Fatigue × Training	3.62 (1.56)	4.00 (1.34)	3.94 (1.41)
Threat × Training × Fatigue	4.11 (1.56)	4.11 (1.41)	4.17 (1.40)
No strategy	2.81 (1.62)	3.85 (1.58)	3.76 (1.54)
Overall	3.53 (1.65)	3.99 (1.42)	3.95 (1.38)

Privacy Protection Behavior

In all waves, we measured participants past privacy behavior. We stated that there are several ways to protect your personal information and privacy on the internet, and then asked participants how often (1 = *Never*, 2 = *Yearly*, 3 = *Monthly*, 4 = *Weekly*, 5 = *Daily*, 6 = *Always*) they: (1) reject to accept cookies when visiting a website, (2) use the cookies settings to only accept necessary cookies, (3) decide not to visit a website because it is only accessible when you accept cookies, (4) delete their cookies, (5) delete their browser history, (6) use the private mode in their browser, (7) use opt-out websites (such as https://www.youronlinechoices.com) to configure whether ads are based on personal data, (8) turn off personalization of services and websites (such as Google and social media), (9) use the "Do Not Track" function of their browser, (10) use a special add-on in their browser (like Ghostery) that make it more difficult for companies to collect data about them, and (11) use an ad blocker. These privacy behaviors were based upon prior studies (e.g., Boerman et al., 2021; Büchi et al., 2017; G. R. Milne et al., 2009; Smit et al., 2014). A factor analysis suggested a three-factor solution with (1) tracking blocking behavior (items 6–11, Cronbach's $\alpha = .80$), (2) rejection of cookies (items 1–3 Cronbach's $\alpha = .78$), (3) deletion of cookies and browser history (items 4–5, Cronbach's $\alpha = .87$).

In wave 1, the past privacy behavior question specified that we were curious about their behavior before their participation to this study. In addition, to be able to test immediate effects, we asked participants how often they intended to do the eleven things in the future. Mean scores of the three factors can be found in Table 3 (intention in wave 1) and Table 4 (past behavior in all waves).

Threat Appraisal

In each wave, we measured perceived susceptibility by asking participants to indicate to what extent they agreed (1 = *Strongly disagree*, 7 = *Strongly agree*) with the

Table 4. Means and Standard Deviations of Privacy Protection Behavior Scores Across the Eight Conditions and the Three Waves.

	Wave 1			Wave 2			Wave 3		
Strategy	Tracking blocking	Cookies rejection	Deletion	Tracking blocking	Cookies rejection	Deletion	Tracking blocking	Cookies rejection	Deletion
Threat	2.41 (1.14)	3.36 (1.36)	3.28 (1.23)	2.52 (1.29)	3.80 (1.18)	3.50 (1.20)	2.48 (1.29)	3.64 (1.25)	3.39 (1.23)
Training	2.10 (1.25)	3.13 (1.41)	3.15 (1.51)	2.79 (1.26)	4.06 (1.06)	3.53 (1.45)	2.79 (1.40)	3.69 (1.28)	3.56 (1.39)
Fatigue	1.86 (1.07)	2.68 (1.43)	2.83 (1.34)	2.28 (1.14)	3.44 (1.36)	3.07 (1.47)	2.11 (1.16)	3.04 (1.34)	2.93 (1.41)
Threat × Training	2.03 (1.26)	3.06 (1.24)	2.89 (1.26)	2.52 (1.37)	3.65 (1.27)	3.15 (1.42)	2.24 (1.20)	3.69 (1.03)	3.38 (1.42)
Threat × Fatigue	2.11 (1.06)	2.99 (1.51)	3.04 (1.44)	2.47 (1.28)	3.81 (1.29)	3.56 (1.56)	2.60 (1.23)	3.53 (1.38)	3.49 (1.45)
Fatigue × Training	2.17 (1.35)	3.14 (1.52)	3.28 (1.51)	2.66 (1.42)	3.93 (1.30)	3.42 (1.52)	2.66 (1.49)	3.75 (1.28)	3.46 (1.47)
Threat × Training × Fatigue	2.28 (1.29)	3.21 (1.38)	3.14 (1.54)	3.11 (1.30)	3.99 (1.26)	3.56 (1.53)	2.89 (1.16)	3.85 (1.26)	3.47 (1.43)
No strategy	2.08 (1.24)	3.25 (1.58)	3.28 (1.58)	2.13 (1.31)	3.40 (1.38)	3.33 (1.40)	2.24 (1.40)	3.57 (1.34)	3.24 (1.35)
Overall	2.13 (1.21)	3.11 (1.44)	3.12 (1.43)	2.55 (1.32)	3.76 (1.28)	3.39 (1.44)	2.50 (1.31)	3.59 (1.29)	3.36 (1.39)

Table 5. Means and Standard Deviations of Perceived Severity and Susceptibility Scores Across Threat Strategy and the Three Waves.

	Wave 1		Wave 2		Wave 3	
Strategy	Perceived severity	Perceived susceptibility	Perceived severity	Perceived susceptibility	Perceived severity	Perceived susceptibility
Threat strategy	5.65 (1.30)	6.15 (0.92)	5.52 (1.29)	5.97 (0.96)	5.24 (1.06)	6.03 (0.96)
No threat	5.58 (1.32)	6.04 (0.82)	5.47 (1.25)	5.84 (0.96)	5.52 (1.17)	5.94 (0.93)
Overall	5.61 (1.31)	6.09 (0.87)	5.49 (1.27)	5.91 (0.96)	5.50 (1.21)	5.98 (0.94)

statements: "I believe that companies collect my personal information and online behavior (such as my name, location, and surfing and searching behavior)," "I believe that companies use my personal data and online behavior to determine what information they show me," and "I believe that companies share my personal information and online behavior with other companies" (based on Boerman et al., 2021). The mean of the three items was used as a measure of perceived susceptibility (Cronbach's $\alpha = .85$). We measured perceived severity with similar items focusing on whether this was perceived as a problem by changing "I believe that. . ." in the statements into "I find it a problem when . . ." (e.g., "I find it a problem when companies collect my personal information and online behavior [such as my name, location, and surfing and searching behavior]"; Boerman et al., 2021; Ham, 2017; Cronbach's $\alpha = .95$).

Coping Appraisal

We measured self-efficacy with the statements: "I am able to protect my personal information and online behavior (such as my name, location, and search and surfing behavior) on the Internet"; "I feel confident that I can secure my privacy on the Internet," and "I can ensure that companies cannot collect my personal information and behavior on the Internet" (Boerman et al., 2021; Cronbach's $\alpha = .85$). Next, we measured response efficacy by asking to what extent (1 = *totally not*, 7 = *totally*) participants believed seven different protection behaviors (i.e., (1) rejecting cookies, (2) only accepting necessary cookies, (3) refraining from visiting a website, (4) deleting cookies, (5) opt-out websites, (6) turning off personalization, (7) using add-ons to prevent tracking) were effective ways to eliminate the collection, usage, and sharing of personal information on the Internet (based on Boerman et al., 2021). A factor analysis suggested a three-factor solution with perceived efficacy of (1) tracking blocking behavior (items 5–7, Cronbach's $\alpha = .89$), (2) rejection of cookies (items 1–3, Cronbach's $\alpha = .78$), and (3) deletion of cookies (item 4).

Privacy Fatigue

We measured individual levels of privacy fatigue using seven items from the scale by Choi et al. (2018), including statements regarding emotional exhaustion and cynicism,

Table 6. Means and Standard Deviations of Perceived Self-Efficacy and Response Efficacy Scores Across Training Strategy and the Three Waves.

	Wave 1				Wave 2				Wave 3			
Strategy	Self-efficacy	Efficacy of tracking blocking	Efficacy of cookies rejection	Efficacy of deletion	Self-efficacy	Efficacy of tracking blocking	Efficacy of cookies rejection	Efficacy of deletion	Self-efficacy	Efficacy of tracking blocking	Efficacy of cookies rejection	Efficacy of deletion
Training	4.65 (1.23)	5.59 (1.08)	5.44 (0.99)	5.52 (1.24)	4.63 (1.18)	5.25 (1.08)	5.32 (1.05)	5.39 (1.32)	4.48 (1.13)	5.11 (1.08)	5.28 (1.01)	5.24 (1.35)
No training	4.34 (1.22)	5.12 (1.05)	5.30 (0.97)	5.44 (1.20)	4.32 (1.22)	5.06 (1.05)	5.22 (1.03)	5.41 (1.25)	4.27 (1.26)	4.94 (1.13)	5.08 (1.10)	5.29 (1.32)
Overall	4.48 (1.24)	5.34 (1.09)	5.37 (0.98)	5.48 (1.21)	4.46 (1.21)	5.15 (1.07)	5.26 (1.04)	5.39 (1.28)	4.37 (1.20)	5.02 (1.11)	5.18 (1.07)	5.27 (1.33)

Table 7. Means and Standard Deviations of Privacy Fatigue Across Fatigue Strategy and the Three Waves.

Strategy	Wave 1	Wave 2	Wave 3
Fatigue strategy	3.82 (1.30)	3.85 (1.21)	3.99 (1.08)
No fatigue strategy	3.73 (1.11)	3.75 (1.15)	3.86 (1.12)
Overall	3.78 (1.12)	3.80 (1.18)	3.92 (1.10)

such as "I am tired of online privacy issues" and "I have become less interested in online privacy issues." The mean of the seven items was used as a measure of individual privacy fatigue (Cronbach's $\alpha = .88$).

Attention Checks

All waves included two attention checks. Participants who failed both checks were redirected to the end of the questionnaire and not included in the data. Following Kees et al. (2017), we included one question saying: "Research shows that people often pay little attention to reading the questions. We therefore want to check if you read this. If you are reading this, please fill out '[answer option]'. What is this study about?" Followed by four answer options. We also included an item in one of the scales asking people to tick a specific answer ("This is a question to test your attention, answer 'Agree' here").

Results

To analyze the data, we conducted (1) ANOVAs to examine immediate effects of the strategies on perceptions and behavioral intentions (in wave 1), and (2) mixed fixed and random effect models in which we allowed random effects of individual participants to examine short- (changes from wave 1 to wave 2) and long-term effects (changes from wave 1 to wave 3). For the analyses, coding, and typesetting, we used R (Version 4.0.3; R Core Team, 2018) and the R-packages car (Version 3.0; Fox & Weisberg, 2019), psych (Version 2.0.12; Revelle, 2021), stats (Version 3.6.2; R Core Team 2018), lme4 (Version 1.1; Bates et al., 2015), and tidyverse (Version 1.3; Wickham et al., 2019). The results are discussed per strategy to address the hypotheses and RQ. For reasons of clarity and conciseness, we mainly focus on significant effects in the description of the results. Tables 3 to 7 present mean scores for the different variables and strategies in the three waves. Tables 8 to 10 shows a summary of effects of the strategies on the three mechanisms, and Tables 11 and 12 show a summary of effects of the strategies on behavioral intentions and the three privacy protection behaviors.

Effect of Threat Strategy

H1 proposed that the threat strategy would increase perceived severity and susceptibility. Results of a one-way ANOVA showed no significant immediate effect of the threat

Table 8. Fixed and Random Effects Models for Effects of the Threat Strategy.

	Perceived severity				Perceived susceptibility			
Fixed effects	Estimated coefficient	*SE*	*t*	*p*	Estimated coefficient	*SE*	*t*	*p*
(Intercept)	5.58	0.08	68.05	<.001	6.04	0.06	101.06	<.001
Wave 2	−0.11	0.07	−1.67	.096	**−0.20**	**0.06**	**−3.63**	**<.001**
Wave 3	−0.06	0.07	−0.92	.360	−0.10	0.06	−1.84	.066
Threat	0.06	0.12	0.55	.586	0.11	0.09	1.29	.199
Wave 2 × Threat	−0.01	0.10	−0.14	.891	0.03	0.08	0.33	.743
Wave 3 × Threat	−0.09	0.10	−0.95	.343	−0.02	0.08	−0.26	.798
Random effects due to respondent	Variance	*SD*			Variance	*SD*		
Intercept	1.05	1.03			0.49	0.70		
Residual	0.54	0.74			0.36	0.60		

Note. Number of observations: 1,395, 465 respondents. Significant effects are in bold.

strategy on perceived severity, $F(1, 463) = 0.27$, $p = .601$. Mixed effects model (see Table 8) showed that perceived severity also did not increase in the short- nor in the long-term in all conditions (see Table 5 for mean differences).

The threat strategy also did not have an immediate effect on perceived susceptibility, $F(1, 463) = 1.86$, $p = .173$. Susceptibility decreased in the short-term, $t(930) = -3.63$, $p < .001$, but this decrease did not depend on the strategy (see Table 5 for means). These effects do not support H1.

Regarding privacy protection behavior (H2), the threat strategy did immediately increase the intention to block tracking (threat strategy $M = 3.77$, $SD = 1.60$, no threat strategy $M = 3.30$, $SD = 1.67$), $F(1, 457) = 10.28$, $p = .001$, but we did not observe an immediate effect of the threat strategy on cookie rejection intention and the intention to delete history and cookies (see Table 11). In addition, the threat strategy did not affect cookie deletion, cookie rejection, nor tracking blocking behavior in wave 2 nor wave 3. Thus, while we find support for an immediate effect of the threat strategy on intention to block tracking (H2a), we do not find support for short- (H2b) and long-term (H2c) effects on privacy protection behavior.

Effect of Training Strategy

H3 proposed that the training strategy would increase self-efficacy and response efficacy. The training strategy was successful at immediately increasing self-efficacy (training $M = 4.65$, no training $M = 4.34$), $F(1, 463) = 7.34$, $p = .007$ (see Table 6). After this increase, self-efficacy did not change in the short- and long-term for all participants (see Table 9).

Table 9. Fixed and Random Effects Models for Effects of Training.

	Self-efficacy				Perceived efficacy of tracking blocking				Perceived efficacy of cookie rejection				Perceived efficacy of cookie deletion			
Fixed effects	Estimated coefficient	*SE*	*t*	*p*	Estimated coefficient	*SE*	*t*	*p*	Estimated coefficient	*SE*	*t*	*p*	Estimated coefficient	*SE*	*t*	*p*
(Intercept)	4.34	0.08	56.80	<.001	5.12	0.07	75.31	<.001	5.30	0.06	81.65	<.001	5.44	0.08	67.43	<.001
Wave 2	−0.02	0.07	−0.32	.751	−0.06	0.07	−0.84	.400	−0.08	0.07	−1.17	.241	−0.03	0.08	−0.38	.702
Wave 3	−0.06	0.07	−0.95	.341	**−0.18**	**0.07**	**−2.51**	**.012**	**−0.22**	**0.07**	**−3.15**	**.002**	−0.15	0.08	−1.77	.077
Training	**0.31**	**0.11**	**2.75**	**.006**	**0.47**	**0.10**	**4.74**	**<.001**	0.14	0.10	1.50	.133	0.08	0.12	0.68	.495
Wave 2 × training	0.00	0.10	0.04	.966	**−0.28**	**0.11**	**−2.65**	**.008**	−0.05	0.10	−0.46	.643	−0.10	0.12	−0.84	.403
Wave 3 × raining	−0.11	0.10	−1.08	.281	**−0.30**	**0.11**	**−2.84**	**.005**	0.06	0.10	0.58	.563	−0.13	0.12	−1.07	.287
Random effects due to respondent	Variance	*SD*			Variance	*SD*			Variance	*SD*			Variance	*SD*		
Intercept	0.89	0.95			0.49	0.70			0.45	0.67			0.75	0.87		
Residual	0.57	0.75			0.66	0.82			0.60	0.78			0.87	0.93		

Note. Number of observations: 1,395, 465 respondents. Significant effects are in bold.

Table 10. Fixed and Random Effects Models for Effects of Fatigue Strategy.

	Privacy fatigue			
Fixed effects	Estimated coefficient	*SE*	*t*	*p*
(Intercept)	3.73	0.07	50.62	<.001
Wave 2	0.01	0.07	0.21	.830
Wave 3	0.13	0.07	1.93	.054
Fatigue	0.08	0.10	0.79	.429
Wave 2 × Fatigue	0.02	0.09	0.18	.854
Wave 3 × Fatigue	0.04	0.09	0.45	.652
Random effects due to respondent	Variance	*SD*		
Intercept	0.78	0.88		
Residual	0.50	0.71		

Note. Number of observations: 1,395, 465 respondents.

Regarding response efficacy, the training strategy was successful at immediately increasing perceived efficacy of tracking blocking behavior (training $M = 5.59$, no training $M = 5.12$), $F(1, 463) = 23$, $p < .001$ (see Table 6). However, perceived efficacy of tracking blocking behavior decreased in the short-term for participants exposed to the training strategy condition (training $M_{wave1} = 5.59$, $M_{wave2} = 5.25$; no training $M_{wave1} = 5.12$, $M_{wave2} = 5.06$; $t(930) = -2.65$, $p = .008$). In the long-term, this decrease was less strong for participants exposed to the training strategy (training $M_{wave1} = 5.59$, $M_{wave3} = 5.11$; no training $M_{wave1} = 5.12$, $M_{wave3} = 4.93$; $t(930) = -2.84$, $p = .005$). Hence, the training mostly increased perceived efficacy of tracking blocking immediately after the intervention, but this effect did not persist in the long-term.

Second, the training strategy did not immediately impact the perceived efficacy of rejecting cookies, $F(1, 463) = 2.47$, $p = .117$. Also, perceived efficacy of rejecting cookies did not change in the short-term, but decreased in the long-term for all participants regardless of exposure to the training strategy, $t(930) = -3.15$, $p = .002$. Hence, the training did not increase perceived efficacy of rejecting cookies.

Third, the training strategy did not impact perceived efficacy of cookie deletion, $F(1, 463) = 0.51$, $p = .474$. The perceived efficacy of deleting cookies also did not change in the short- nor long-term (see Table 9). Thus, our results offer partial support for H3a for immediate effects on self-efficacy and perceived efficacy of tracking blocking behavior, but no support for H3b and H3c as these effects did not persist.

Regarding privacy protection behavior (H4), a one-way ANOVA revealed a main effect of the training strategy on the intention to block tracking (training $M = 3.93$, no training $M = 3.18$), $F(1, 457) = 27.15$, $p < .001$. The training strategy also resulted in increased tracking blocking behavior in the short-term (training $M_{wave1} = 2.15$, $M_{wave2} = 2.77$; no training $M_{wave1} = 2.13$, $M_{wave2} = 2.36$; $t(930) = 3.06$, $p = .002$) and in the

Table 11. Three-Way ANOVA for Privacy Protection Intention.

	Tracking blocking intention					Cookie rejection intention					Deletion intention				
	Sum of squares	*df*	Mean square	*F*	*p*	Sum of squares	*df*	Mean square	*F*	*p*	Sum of squares	*df*	Mean square	*F*	*p*
Threat	**25.8**	**1**	**25.84**	**10.28**	**.001**	2.4	1	2.42	1.20	.274	5.5	1	5.50	2.95	.086
Training	**68.2**	**1**	**68.24**	**27.15**	**<.001**	**8.7**	**1**	**8.68**	**4.30**	**.039**	**12.7**	**1**	**12.74**	**6.84**	**.009**
Fatigue	0.8	1	0.78	0.31	.578	1.2	1	1.24	0.61	.434	1	1	1.00	0.54	.463
Threat × Training	5.1	1	5.11	2.03	.155	4.3	1	4.30	2.13	.150	5.8	1	5.76	3.09	.079
Threat × Fatigue	4.4	1	4.38	1.74	.187	3.9	1	3.87	1.92	.167	**7.6**	**1**	**7.60**	**4.08**	**.044**
Fatigue × Training	4.6	1	4.64	1.85	.175	0.1	1	0.11	0.06	.815	0.1	1	0.09	0.05	.830
Threat × Training × Fatigue	0	1	0.02	0.01	.934	0.1	1	0.13	0.06	.801	0.1	1	0.07	0.04	.846
Residual	1,148.9	457	2.51			923.1	457	2.02			850.5	457	1.86		

Note. Significant effects are in bold.

Table 12. Fixed and Random Effects Models for Privacy Protection Behaviors.

	Tracking blocking				Cookie rejection				Deletion of cookies and browser history			
Fixed effects	Estimated coefficient	*SE*	*t*	*p*	Estimated coefficient	*SE*	*t*	*p*	Estimated coefficient	*SE*	*t*	*p*
(Intercept)	2.08	0.16	12.92	<.001	3.25	0.17	18.86	<.001	3.28	0.18	18.22	<.001
Wave 2	0.06	0.14	0.41	.686	0.16	0.16	0.97	.332	0.05	0.12	0.40	.688
Wave 3	0.16	0.14	1.14	.256	**0.33**	**0.15**	**2.13**	**.033**	−0.04	0.12	−0.33	.738
Threat	0.33	0.22	1.51	.133	0.11	0.23	0.48	.630	−0.00	0.25	−0.02	.987
Training	0.03	0.23	0.11	.910	−0.12	0.25	−0.48	.629	−0.13	0.26	−0.51	.610
Fatigue	−0.22	0.23	−0.95	.342	**−0.57**	**0.24**	**−2.38**	**.018**	−0.45	0.25	−1.77	.077
Threat × Training	−0.40	0.33	−1.22	.221	−0.18	0.35	−0.53	.600	−0.26	0.37	−0.69	.490
Threat × Fatigue	−0.08	0.32	−0.26	.796	0.21	0.33	0.61	.540	0.21	0.36	0.59	.554
Fatigue × Training	0.28	0.33	0.86	.392	0.59	0.34	1.71	.088	0.58	0.37	1.59	.113
Threat × Training × Fatigue	0.27	0.47	0.57	.570	−0.07	0.49	−0.15	.881	−0.08	0.52	−0.16	.876
Wave 2 × Threat (H2)	0.05	0.19	0.30	.766	0.29	0.21	1.37	.170	0.18	0.17	1.05	.292
Wave 3 × Threat (H2)	−0.08	0.19	−0.41	.683	−0.04	0.21	−0.20	.843	0.16	0.17	0.96	.337
Wave 2 × Training (H4)	**0.63**	**0.21**	**3.06**	**.002**	**0.77**	**0.22**	**3.47**	**<.001**	0.33	0.18	1.87	.062
Wave 3 × Training (H4)	**0.53**	**0.21**	**2.56**	**.011**	0.23	0.22	1.03	.304	**0.46**	**0.18**	**2.58**	**.010**
Wave 2 × Fatigue (H6)	0.36	0.20	1.78	.075	**0.61**	**0.22**	**2.79**	**.005**	0.19	0.17	1.09	.277
Wave 3 × Fatigue (H6)	0.09	0.20	0.44	.663	0.04	0.22	0.18	.860	0.14	0.17	0.80	.422
Wave 2 × Threat × Training	−0.26	0.29	−0.88	.381	−0.62	**0.32**	**−1.97**	**.049**	−0.30	0.25	−1.18	.239
Wave 3 × Threat × Training	−0.40	0.29	−1.26	.174	0.12	0.32	0.39	.700	−0.09	0.25	−0.35	.724
Wave 2 × Threat × Fatigue	−0.11	0.28	−0.40	.687	−0.24	0.30	−0.79	.432	0.09	0.24	0.35	.723
Wave 3 × Threat × Fatigue	0.32	0.28	1.13	.257	0.21	0.30	0.68	.500	0.20	0.24	0.81	.418
Wave 2 × Fatigue × Training	−0.55	0.29	−1.91	.056	**−0.75**	**0.31**	**−2.41**	**.016**	−0.42	0.25	−1.69	.092
Wave 3 × Fatigue × Training	−0.28	0.29	−0.97	.335	0.01	0.31	0.03	.975	−0.37	0.25	−1.50	.133
Wave 2 × Threat × Training × Fatigue	0.65	0.41	1.57	.118	0.58	0.45	1.28	.199	0.30	0.36	0.84	.403
Wave 3 × Threat × Training × Fatigue	0.27	0.41	0.66	.510	−0.25	0.45	−0.55	.582	−0.12	0.36	−0.35	.727
Random effects due to respondent	Variance	*SD*			Variance	*SD*			Variance	*SD*		
Intercept	0.96	0.98			1.02	1.01			1.52	1.23		
Residual	0.61	0.78			0.72	0.85			0.46	0.68		

Note. Number of observations: 1,395, 465 respondents. . Significant effects are in bold.

long-term (training $M_{wave1} = 2.15$, $M_{wave3} = 2.66$; no training $M_{wave1} = 2.13$, $M_{wave3} = 2.36$; $t(930) = 2.56$, $p = .011$). This shows a positive impact of the training strategy immediately on tracking blocking intention and on behavior in the short- and long-term.

Second, regarding cookies rejection, we observed a main effect of the training strategy on the intention to do so at wave 1: participants exposed to the training strategy showed slightly more intention to reject cookies (training $M = 4.13$, no training $M = 3.87$), $F(1, 457) = 4.30$, $p = .039$. Regarding change in this behavior over time, the training strategy also resulted in increased cookie rejection behavior in the short-term (training $M_{wave1} = 3.14$, $M_{wave2} = 3.92$; no training $M_{wave1} = 3.08$, $M_{wave2} = 3.62$; $t(930) = 3.47$, $p = .001$), but no changes were observed in the long-term. This shows a positive impact of the training strategy on cookie rejection intention immediately after the intervention and on the behavior in the short-term, but not in the longer term.

Third, we observed a main effect of the training strategy on the intention to delete cookies and history at wave 1 (training $M = 4.12$, no training $M = 3.80$), $F(1, 457) = 6.84$, $p = .009$. In addition, the training strategy did not lead to more deletion behavior in the short-term, but the training did result in increased cookie deletion behavior in the long-term (training $M_{wave1} = 3.12$, $M_{wave3} = 3.47$; no training $M_{wave1} = 3.11$, $M_{wave2} = 3.26$; $t(930) = 2.58$, $p = .010$). Overall, the results show full support for H4 for tracking blocking, support H4a and H4b for cookie rejection, and support H4a and H4c for cookie deletion.

Effect of Privacy Fatigue Strategy

H5 proposed that the privacy fatigue strategy would decrease privacy fatigue in the short- and long-term. The strategy aimed at combating fatigue did not influence privacy fatigue immediately at wave 1, $F(1, 463) = 0.64$, $p = .424$ (see Table 7 for means). Fatigue also did not change in the short- nor long-term independent of condition (see Table 10). These findings do not support H5.

Regarding the impact of privacy fatigue strategy on privacy protection behavior (H6), we did not observe an effect on the intention to block tracking at wave 1, nor on the tracking blocking behavior in the short- and long-term. For cookie rejection, we did not observe an immediate effect on intention, but a significant effect in the short-term, meaning that cookie rejection behavior increased slightly more for participants exposed to the fatigue strategy (fatigue strategy $M_{wave1} = 3.00$, $M_{wave2} = 3.79$; no fatigue $M_{wave1} = 3.21$, $M_{wave2} = 3.73$; $t(930) = 2.79$, $p = .005$). In the long-term, there was no change in this behavior in all conditions. Finally, regarding intention to delete cookies and history, we did not observe a main effect of the fatigue strategy. There were also no changes in deletion behavior in the short- nor long-term independent of condition. Thus, the fatigue strategy increased cookie rejection only in the short-term. These findings support H6b for cookie rejection behavior, but do not support H6a and H6c.

Effect of Combinations of the Strategies

RQ1 asked what combination of strategies is most effective in fostering privacy protection behavior. Regarding intentions measured at wave 1, we observed a significant

interaction between the threat and fatigue strategy on cookie and history deletion intention, $F(1, 457) = 4.08$, $p = .044$ (see Table 11). While threat and fatigue do not significantly impact the intention independently, a combination of these strategies does.

Regarding privacy protection behavior, we observed a significant interaction between the training and fatigue strategies in the short-term (wave 2) for cookie rejection behavior, $t(930) = -2.41$, $p = .016$ (see Table 12). While both fatigue and training on their own increased cookie rejection behavior, the combination of these strategies had the strongest effect in the short-term. This interaction effect did not occur in the long-term ($p = .975$). Hence, we can conclude that combining combating fatigue and training is more effective for certain behaviors in the short-term.

Furthermore, we observed an interaction between the training and the threat strategies on cookie rejection behavior in the short-term, $t(930) = -1.97$, $p = .049$ (see Table 12). More specifically, the threat strategy decreased the effectiveness of training at wave 2 (increase was largest when the training was not combined with other strategies, see Table 4 for means). Hence, we can conclude that making privacy threats salient decreases the effectiveness of training certain behaviors.

Discussion

To empower internet users and improve their resilience, this study aimed to gain insights into which (combination of) intervention strategies most effectively increase(s) privacy protection behavior. Based upon prior research, we know that knowledge interventions may not always have the anticipated empowering effect (Strycharz et al., 2019, 2021). Therefore, we argue that an intervention designed to help people to protect their privacy should focus on other factors than just knowledge. Drawing upon Protection Motivation Theory (Rogers, 1975; Witte, 1992), we proposed, developed, and examined the immediate, short- and long-term effects of (combinations) of three intervention strategies: (1) increasing awareness of the threat to privacy, (2) training effective privacy protection behavior, and (3) addressing and combating privacy fatigue. The study's longitudinal approach contributes to our understanding of which strategies can effectively empower people to protect their privacy in the long-term.

Results showed that the training strategy was able to achieve its anticipated effect. Teaching internet users how to take specific actions to protect their privacy increased perceived self-efficacy to combat the threat and the perceived efficacy of the privacy protection measures included in the training. Moreover, the training strategy increased privacy protection behaviors. In particular, the training strategy immediately increased intentions to block tracking, reject cookies, and delete cookies and browser history. In addition, the training positively impacted tracking blocking behavior in the short- and long-term, actual cookie rejection in the short term (2 weeks later), and deletion behavior in the long-term (2 months later). This means that the most effective behavior to safeguard privacy (blocking tracking) was effectively trained and this effect persisted over time. The short-term effect on cookie rejection shows that the training came across, but that this effect wears off. This may be explained by the temporal costs of

these protective behaviors. While blocking tracking involves one-time action (e.g., installing a tracking blocker), rejecting cookies requires repeated effort from the individual (i.e., rejecting cookies whenever they visit a new website with a cookie consent request or cookie wall), possibly causing higher costs of this action. As past research on PMT has shown, the more negative the protective action is experienced, the less motivated users are to execute it (S. Milne et al., 2000), which possibly explains the wear-off effect for rejecting cookies.

Furthermore, we find that the other intervention strategies did not have the anticipated effects. The strategy aimed to increase the threat appraisal (threat strategy) did not increase perceived severity and susceptibility, and the strategy combating fatigue (fatigue strategy) did not diminish privacy fatigue. The threat strategy did cause an immediate increase in intentions to block tracking and the fatigue strategy only had a short-term effect on cookie rejection behavior.

Moreover, results show that some combinations of strategies cause a potential synergy effect but also diminish the effectiveness of strategies. In particular, our findings demonstrate that while the threat and privacy fatigue strategies do not significantly impact the intention to delete cookies and browser history independently, a combination of these strategies does. In addition, combining the fatigue and the training strategy increases cookie rejection in the short-term more than the strategies do on their own. However, making privacy threats salient (i.e., the threat strategy) seems to decrease the effectiveness of the training on cookie rejection behaviors. This means that an intervention that aims to empower users to protect their privacy by having them reject tracking cookies should include both the actual training of privacy protection behaviors *and* diminish feelings of privacy fatigue to maximize short-term effects.

Theoretical Implications

This study reiterates the relevance of the PMT in the context of online privacy, as asserted in previous studies (e.g., Boerman et al., 2021; Dienlin & Metzger, 2016; Ioannou et al., 2021; Strycharz et al., 2019). The PMT proposes the importance of both the threat appraisal and the coping appraisal in protection motivation. Our findings indicate that the effectiveness of our strategies mostly relied on the influence on the coping appraisal, rather than the threat appraisal. Especially self-efficacy scores were rather low (overall mean scores range between 4.37 and 4.46 in the three waves), indicating that people are not very confident in their ability to protect their privacy. Additionally, the finding that especially the training effectively influences the coping appraisal (i.e., self- and response-efficacy) and ultimate privacy protection, emphasizes earlier claims that increasing skills and literacy is an effective way to empower people to protect their privacy (Büchi et al., 2017; Masur, 2020; Park, 2013).

Moreover, the threat strategy did not seem effective in our study, most likely because there was not much to win when it comes to the threat appraisal. The means of both perceived severity and susceptibility were consistently high in all waves (overall mean scores range between 5.49 and 6.09), indicating a possible ceiling effect. In line with previous work (Boerman et al., 2021), these means suggest that the perceived

threat to online privacy is already high. People may thus not require interventions to make them aware of the threats to their privacy, but rather they need to learn how to protect themselves.

Finally, our research demonstrates the importance of countering resistance and digital resignation by combating privacy fatigue. Although addressing only fatigue does not influence perceived fatigue or most privacy protection behaviors, our research does suggest that addressing privacy fatigue could strengthen the effectiveness of the training, in particular by increasing the rejection of tracking cookies. This demonstrates the importance of focusing not only on cognitive, motivation-driven behavior, but also on less rational, more intuitive states (such as privacy fatigue) within the context of online privacy.

Practical Implications

As previous research showed no effect of interventions focusing on increasing technical or legal knowledge, this study makes a first step in unraveling which intervention strategies could work. Although the found effects are not very large (i.e., differences never exceed the one-point difference), the results give hope that a training that teaches how to perform effective privacy protection behavior could empower consumers and motivate and enable them to protect their privacy. Providing a training can effectively boost people's confidence (i.e., increase self-efficacy) and change privacy protection behavior, even in the long-term.

The interventions were specifically designed to resemble existing tools and toolkits online (such as the Fix Your Privacy Tool Kit by Bits of Freedom, https://www.fixjeprivacy.nl). Thus, these type of online training interventions could be easily implemented in existing media and digital literacy programs and made available on platforms of consumer and privacy organizations such as Bits of Freedom and Privacy Rights Clearinghouse. Furthermore, our study suggests that the effectiveness of such trainings can be boosted by also addressing the more emotional and intuitive factor of privacy fatigue.

Limitations and Future Research

Although we paid a lot of attention to the development of our strategies, both the threat and fatigue strategies did not have the anticipated effects. The ineffectiveness of the threat strategy could be due to a ceiling effect, however, this is not true for the fatigue strategy. The mean scores of privacy fatigue could certainly be improved, however, unfortunately, our strategy did not achieve this goal. As privacy fatigue overall encompasses the feeling of uselessness and powerlessness, and the idea that privacy protection is futile, and based upon the information provided by our participants in the pretests, we decided to focus on emphasizing that protecting your privacy is both simple and effective. However, the text and examples used in our strategy did not seem to work sufficiently. Future research could further examine what strategies do diminish people's feelings of privacy fatigue.

Furthermore, our intervention strategies were not mobile friendly and some of the training steps were specifically designed for desktop browsers. As online privacy does not only concern desktop users and extends to mobile phones, further research could develop mobile friendly versions of the intervention strategies and test their effectiveness.

In addition, privacy protection behavior was measured via self-report, which has the limitation of under- or overestimation of behavior. Additionally, our longitudinal approach required us to repeat these questions, making our participants more familiar with the questions, which may have led to more social desirable answers. Nevertheless, our data do not point in this direction, as more social desirable answers would have increased privacy protection behaviors, which was not the case.

Finally, in this study we did not investigate whether the effects of the strategies vary between different contexts and groups of people. The current study has been conducted in the Netherlands, a member of the European Union in which the General Data Protection Regulation is in power. This regulation's aims are to set high standards for the collection and processing of personal data as well as enhance consumer empowerment. As a result, GDPR impacts how data collection on the web is designed, what data are collected, how users are informed about these practices and what rights they have (Degeling et al., 2019). This might mean that while in the Netherlands training privacy behaviors is effective in increasing protection behavior, this may be different in countries in which consumers are offered less information and privacy rights. Hence, future research could examine the interventions in a non-GDPR context. Furthermore, research has shown that there are important differences between people, making some of them more vulnerable to privacy threats than others (e.g., Kezer et al., 2016; Tifferet, 2019) and emphasize the existence of new digital divides, not universal, but created by the context of online data collection (Helberger et al., 2021). Factors that influence vulnerability are among others age (Kezer et al., 2016), gender (Tifferet, 2019), and data collection context (Matz et al., 2020). Future research should examine whether intervention strategies that are more tailored to personal characteristics, needs, skills, and context of data collection could be more effective in boosting the resilience of individuals.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was funded by the SIDN fund (https://www.sidnfonds.nl/projecten/hoe-kun-je-mensen-motiveren-om-hun-data-de-baas-te-zijn).

ORCID iDs

Sophie C. Boerman https://orcid.org/0000-0002-2453-1493

Joanna Strycharz https://orcid.org/0000-0001-7739-3349

Edith G. Smit https://orcid.org/0000-0002-6913-4897

References

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

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1–21. https://doi.org/10.1016/j.im.2015.08.001

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bates D., Mächler M., Bolker B., & Walker S. (2015). Fitting Linear Mixed-Effects Models Using lme4. *Journal of Statistical Software*, *67*(1), 1–48. doi:10.18637/jss.v067.i01.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of internet skills for online privacy protection. *Information, Communication & Society*, *20*, 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, 52, 167–182. doi:10.1109/TPC.2009.2017985

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy. . . Now take some cookies-measuring the GDPR's impact on web privacy. *Informatik Spektrum*, *42*(5), 345–346. https://doi.org/10.14722/ndss.2019.23378

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, *110*, 106382. https://doi.org/10.1016/j.chb.2020.106382

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of*

Computer-mediated Communication, *12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Fox, J., & Weisberg, S. (2019). *An R companion to applied regression* (3rd ed.). Sage.

Fransen, M. L., Verlegh, P. W., Kirmani, A., & Smit, E. G. (2015). A typology of consumer strategies for resisting advertising, and a review of mechanisms for countering them. *International Journal of Advertising*, *34*(1), 6–16. https://doi.org/10.1080/02650487.2014.995284

Gibbs, J. L., Ellison, N. B., & Lai, C. H. (2011). First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, *38*(1), 70–100. https://doi.org/10.1177/0093650210377091

Ham, C. D. (2017). Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising*, *36*(4), 632–658. https://doi.org/10.1080/02650487.2016.1239878

Ham, C. D., & Nelson, M. R. (2016). The role of persuasion knowledge, assessment of benefit and harm, and third-person perception in coping with online behavioral advertising. *Computers in Human Behavior*, *62*, 689–702. https://doi.org/10.1016/j.chb.2016.03.076

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757.

Helberger, N., Lynskey, O., Micklitz, H. W., Rott, P., Sax, M., & Strycharz, J. (2021). EU consumer protection 2.0. *BEUC*. https://uol.de/f/2/dept/wire/fachgebiete/arbeitsrecht/Aufsaetze/BEUC_EU_Consumer_Protection_2.0.pdf

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), 7. https://doi.org/10.5817/CP2016-4-7

Ioannou, A., Tussyadiah, I., & Marshan, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. *Psychology & Marketing*, *38*(10), 1766–1778. https://doi.org/10.1002/mar.21529

Jacks, J. Z., & Cameron, K. A. (2003). Strategies for resisting persuasion. *Basic and Applied Social Psychology*, *25*(2), 145–161. https://doi.org/10.1207/S15324834BASP2502_5

Kane, G. C., Alavi, M., Labianca, G., & Borgatti, S. P. (2014). What's different about social media networks? A framework and research agenda. *MIS Quarterly*, *38*(1), 275–304. https://doi.org/10.25300/MISQ/2014/38.1.13

Kees, J., Berry, C., Burton, S., & Sheehan, K. (2017). An analysis of data quality: Professional panels, student subject pools, and Amazon's Mechanical Turk. *Journal of Advertising*, *46*(1), 141–155. https://doi.org/10.1080/00913367.2016.1269304

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1), 2. https://doi.org/10.5817/CP2016-1-2

Knowles, E., & Linn, J. A. (2004). Approach-avoidance model of persuasion: Alpha and omega strategies for change. In E. Knowles & J. A. Linn (Eds.), *Resistance and persuasion* (pp. 117–148). Lawrence Erlbaum Associates Publishers.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, *22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Matz, S. C., Appel, R. E., & Kosinski, M. (2020). Privacy in the age of psychological targeting. *Current Opinion in Psychology*, *31*, 116–121. https://doi.org/10.1016/j.copsyc.2019.08.010

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

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

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

R Core Team. (2018). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing.

Revelle, W. (2021). *psych: Procedures for psychological, psychometric, and personality research*. Northwestern University.

Robinson, C. (2017). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569–582. https://doi.org/10.1016/j.tele.2016.09.006

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). Guilford.

Selwyn, N., & Pangrazio, L. (2018). Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data & Society*, *5*(1), 2053951718765021. https://doi.org/10.1177/2053951718765021

Slater, M. D., Hayes, A. F., & Chung, A. H. (2015). Injury news coverage, relative concern, and support for alcohol-control policies: An impersonal impact explanation. *Journal of Health Communication*, *20*(1), 51–59. https://doi.org/10.1080/10810730.2014.906523

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15–22. https://doi.org/10.1016/j.chb.2013.11.008

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *It Professional*, *18*(5), 26–32. https://doi.org/10.1109/MITP.2016.84

Strycharz, J., Smit, E. G., Helberger, N., & van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior*, *120*, 106750. https://doi.org/10.1016/j.chb.2021.106750

Strycharz, J., Van Noort, G., Smit, E. G., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *13*(2), 1. https://doi.org/10.5817/CP2019-2-1

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, *93*, 1–12. https://doi.org/10.1016/j.chb.2018.11.046

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media & Society*, *9*(2), 300–318. https://doi.org/10.1177/1461444807072219

Tyler, T. R., & Cook, F. L. (1984). The mass media and judgments of risk: Distinguishing impact on personal and societal level judgments. *Journal of Personality and Social Psychology*, *47*(4), 693. https://doi.org/10.1037/0022-3514.47.4.693

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

Westin, A. (1967). *Privacy and freedom*. Atheneum.

Wickham, H. (2017). *Tidyverse: Easily install and load 'tidyverse' packages*. https://CRAN.R-project.org/package=tidyverse

Wickham, H., Averick, M., Bryan, J., Chang, W., McGowan, L. D., François, R., Grolemund, G., Hayes, A., Henry, L., Hester, J., Kuhn, M., Pedersen, T. L., Miller, E., Bache, S. M., Müller, K., Ooms, J., Robinson, D., Seidel, D. P., Spinu, V., . . . Yutani, H. (2019). Welcome to the tidyverse. *Journal of Open Source Software*, *4*(43), 1686. https://doi.org/10.21105/joss.01686

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books Ltd.

Author Biographies

Sophie C. Boerman (PhD, University of Amsterdam) is associate professor of persuasive communication in the Strategic Communication group at Wageningen University & Research. Her research addresses how people are influenced by (digital) communication, and how persuasive communication can empower people to make informed, healthy, and sustainable decisions.

Joanna Strycharz (PhD, University of Amsterdam) is assistant professor in the Amsterdam School of Communication Research (ASCoR), University of Amsterdam. She studies personalized advertising, its impact on consumers, their privacy, and consumer empowerment.

Edith G. Smit (PhD, University of Amsterdam) is a full professor and chair of Persuasion & Consumer Empowerment, Amsterdam School of Communication Research (ASCoR), University of Amsterdam.