Exploring motivations for online privacy protection behavior: Insights from panel data

Boerman, S.C.; Kruikemeier, S.; Zuiderveen Borgesius, F.J.

DOI
10.1177/0093650218800915

Publication date
2021

Document Version
Final published version

Published in
Communication Research

License
CC BY-NC

Link to publication

Citation for published version (APA):
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

Article

Communication Research
2021, Vol. 48(7) 953–977

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0093650218800915
journals.sagepub.com/home/crx
SAGE

Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data

Sophie C. Boerman[1], Sanne Kruikemeier[1], and Frederik J. Zuiderveen Borgesius[1]

Abstract
Personally managing and protecting online privacy has become an essential part of everyday life. This research draws on the protection motivation theory (PMT) to investigate privacy protective behavior online. A two-wave panel study (*N* = 928) shows that (1) people rarely to occasionally protect their online privacy and (2) people most often delete cookies and browser history or decline cookies to protect their online privacy. In addition, (3) the perceived threat is high: People perceive the collection, usage, and sharing of personal information as a severe problem to which they are susceptible. The coping appraisal is mixed: Although people do have confidence in some protective measures, they have little confidence in their own efficacy to protect their online privacy. Moreover, privacy protective behavior is affected by perceived severity and response efficacy. These findings emphasize the relevance of the PMT in the context of privacy threats, and have important implications for regulators.

Keywords
privacy, protective behavior, protection motivation theory, cookies, ad blockers, Internet, computer-mediated communication, survey, panel data

Introduction

People spend a growing amount of their time online, leaving more and more personal information online. Disclosing information online has benefits, for instance, it helps to

[1]University of Amsterdam, The Netherlands

Corresponding Author:
Sophie C. Boerman, Amsterdam School of Communication Research, University of Amsterdam, P.O. Box 15791, 1001 NG Amsterdam, The Netherlands.
Email: S.C.Boerman@uva.nl

establish and maintain social connections (Gibbs, Ellison, & Lai, 2011; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). In addition, tracking and using personal information can also improve website usability, convenience, and efficiency; and enables companies to personalize services and messages (e.g., online behavioral advertising [OBA] and political microtargeting; Boerman, Kruikemeier, & Zuiderveen Borgesius, 2017; Buchanan, Paine, Joinson, & Reips, 2007; Estrada-Jiménez, Parra-Arnau, Rodríguez-Hoyos, & Forné, 2017).

However, these benefits go together with a risk to people's (informational) privacy. An important aspect of informational privacy is individual control over the collection and dissemination of personal information (Baruh, Secinti, & Cemalcilar, 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). As companies collect, use, and share personal information that is available online, people often lose control over their personal data. As a result, people are concerned about their online privacy, worry about possible misuse of their personal information, and express the desire to have more control over their personal information online (e.g., Gomez, Pinnick, & Soltani, 2009; Smit, Van Noort, & Voorveld, 2014; Turow, King, Hoofnagle, Bleakley, & Hennessy, 2009). Consequently, personally managing and protecting online privacy has become an essential part of everyday life (Büchi, Just, & Latzer, 2017).

Self-management of online privacy seems particularly important as the law only provides limited privacy protection. First, in many countries, the law is not fully prepared for modern data processing practices. Even if lawmakers and regulators want to protect privacy, they are struggling with the question of how to provide effective legal privacy protection. Moreover, even if up-to-date privacy laws are in place, enforcement is often insufficient. Regulators have limited resources to make companies comply with the law.

Second, in many countries, privacy law partly delegates the responsibility of privacy protection to users (Zuiderveen Borgesius, 2015; Baruh & Popescu, 2017). Privacy laws and regulators focus heavily on transparency and consumer empowerment. Roughly summarized, many laws allow companies to collect, use, and disclose data, as long as they provide transparency about these practices, and ask the consumer's consent for the data use. For example, in the European Union (EU), people can provide a company a legal basis for using their personal data, by consenting to such use (EU General Data Protection Regulation, 2016, article 6). And, EU law only allows companies to use tracking cookies and similar technologies after prior consent of the Internet user (EU ePrivacy Directive, 2009). In the United States, informed consent plays an important role in privacy law too. For instance, "companies should obtain consumers' affirmative express consent before collecting sensitive data" (Federal Trade Commission, 2012, p. 58).

This means that laws mainly focus on consumers' consent, and lawmakers appear to assume that empowered consumers can make rational, educated decisions in their own best interest. The question, however, is whether people are actually empowered and able to make decisions about giving consent and to protect their online privacy after giving consent. When this would not be the case, it would suggest a need for more effective privacy laws, which rely less on empowering consumers, and more on protecting them. Prior research reveals that people generally do try to protect their privacy online (e.g., Büchi et al., 2017; McDonald & Cranor, 2010; Smit et al., 2014). However, studies into privacy protective behavior are difficult to compare as they measured varying behaviors. In addition, these studies rarely include tracking prevention tools, ad blockers, Do Not Track functions in a browser, or opt-out websites (Chanchary, Abdelaziz, & Chiasson, 2018; Helsloot, Tillem, & Erkin, 2017). This had led to a call for research that considers a wider diversity of types of privacy protective behavior (Baruh et al., 2017). This study aims to answer this call by investigating whether people protect their online privacy and which measures they take.

Furthermore, there is a need to understand which factors explain whether people protect their online privacy. Understanding why people do (or do not) protect their online privacy could help to develop interventions that can create awareness, empower people, and help them to change their behavior when necessary. Research has shown that protective behavior depends on people's privacy concerns and attitudes, knowledge, skills, experience, education, gender, and age (e.g., Baruh et al., 2017; Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009; Smit et al., 2014). However, research into online privacy protective behavior often lacks a theoretical foundation. Where most prior research draws on the communication privacy management theory (Petronio, 2002) and privacy calculus model (e.g., Dienlin & Metzger, 2016; Krasnova et al., 2010), the present study draws on the protection motivation theory (PMT) to investigate the extent to which threat and coping appraisals influence protective behavior. The PMT posits that people are motivated to protect themselves against a threat when they believe the threat is severe and real (i.e., perceived threat), and when they feel confident that they can protect themselves and feel that their response is effective (i.e., perceived efficacy; Rogers, 1975). The PMT is particularly relevant in the context of online privacy as it can identify which factors may withhold people from engaging in protective behavior.

Altogether, the aim of this article is to gain insights into (1) whether people protect their online privacy, (2) which methods they use most often, and (3) what factors of the PMT may explain protective behavior. We investigate these three subjects with a large-scale panel study with two waves ($N = 928$).

Online Privacy Protection Behavior

People can try to protect their online privacy in various ways. Protective behaviors are defined as "specific computer-based actions that consumers take to keep their information safe" (Milne, Labrecque, & Cromer, 2009, p. 450). People can protect their online privacy by limiting the information that they share, and by adopting privacy protective measures (Baruh et al., 2017; Büchi et al., 2017). A meta-analysis of several studies concerning online privacy showed that these two behaviors do not seem to be related (Baruh et al., 2017). For instance, people who protect their online privacy on social network sites, do not necessarily also limit self-disclosure (Chen & Chen, 2015). In this study, we focus on *what people actively do to mitigate the collection, usage,* *and sharing of their personal information to protect their online privacy*. These behaviors include installing an ad blocker, cookie management, and using the private mode and Do Not Track functions in a browser. This study excludes practices that limit information sharing, such as refraining from disclosing personal information (Chai et al., 2009; LaRose & Rifon, 2007), "untagging" posts or photos (Dienlin & Metzger, 2016), and changing privacy settings in social network sites (Chen & Chen, 2015; Walrave, Vanwesenbeeck, & Heirman, 2012). It also excludes other behavior that does not directly mitigate the collection, usage, and sharing of their personal information such as refraining from reading unsolicited emails and sending negative messages to companies sending unsolicited emails (Moscardelli & Divine, 2007; Sheehan & Hoy, 1999; Youn & Hall, 2008).

Several cross-sectional studies have examined people's protective behavior and revealed that people generally do try to protect their privacy online (e.g., Büchi et al., 2017; Chanchary et al., 2018; McDonald & Cranor, 2010; Smit et al., 2014). However, because the studies measure different behaviors, and some do not provide descriptive statistics of the protective behaviors, there is no clear overview of the occurrence of different methods that people use to protect their online privacy. In addition, their results vary: Some find that clearing cookies is the top practice (Büchi et al., 2017; Chanchary et al., 2018), whereas others find that installing virus checkers and scanning for spyware is used more often (Milne et al., 2009; Smit et al., 2014).

Furthermore, many studies focus on people's privacy protection on social networking sites, such as Facebook (e.g., Chen & Chen, 2015; Dienlin & Metzger, 2016; Dienlin & Trepte, 2015; Feng & Xie, 2014; Walrave et al., 2012). Privacy threats, however, apply to the Internet as a whole and are not restricted to social networking sites. To gain a better understanding of people's protective behavior in general, and of the extent to which people use various methods, we pose the following research question:

> **Research Question 1:** To what extent do people protect their online privacy? And, which methods are used most often?

Predicting Privacy Protective Behavior Using the PMT

Next to gaining insights into people's actual protective behavior, we aim to predict why people protect their online privacy. Previous research has already demonstrated the importance of privacy concerns and attitudes. People who are more concerned about their privacy, and who place high importance on their personal privacy are more likely to engage in protective behavior (e.g., Baruh et al., 2017; Büchi et al., 2017; Chai et al., 2009; Dienlin & Trepte, 2015; Ham, 2017; Moscardelli & Divine, 2007; Smit et al., 2014). In addition, individual's knowledge, skills, and experience also play a role. People who have more Internet skills, more technical knowledge, and more knowledge about OBA are more likely to engage in privacy protection (Baruh et al., 2017; Buchanan et al., 2007; Büchi et al., 2017; Ham, 2017; Ham & Nelson, 2016; Malandrino, Scarano, & Spinelli, 2013; Park, 2013). In addition, having more experience with privacy violations increases protective behavior (Büchi et al., 2017; Chai et al., 2009). These findings suggest that people with less knowledge, skills, and experience are more vulnerable to privacy threats. This is of particular importance as research has shown that there are large differences in digital skills between people (i.e., digital inequality; Hargittai & Hinnant, 2008).

Although previous work provided important insights into predictors of privacy protection, these studies often lack a theoretical background. Some studies draw on communication privacy management theory (e.g., Baruh et al., 2017; Metzger, 2007) and privacy calculus model (e.g., Dienlin & Metzger, 2016; Krasnova et al., 2010) to understand online privacy. Both these theories claim that people make rational decisions about their private information. In short, the communication privacy management theory proposes that people believe that they have the right to control their private information and create rules about who is denied or granted access to specific information (Petronio, 2002). In these rules, there is a tension between social and private goals. The privacy calculus model suggests that people decide how much they want to disclose about themselves based on the perceived benefits (e.g., self-expression) and the perceived costs (e.g., privacy concerns): When the benefits outweigh the costs, people are usually more inclined to disclose information.

To gain more insight into why people protect their privacy online, we draw on the PMT (Rogers, 1975; Witte, 1992). With respect to the communication privacy management theory and privacy calculus model, the PMT adds the component of individual efficacy. Rather than focusing on the reasons (not) to disclose private information, the theory provides a framework to understand both whether people perceive a threat in the first place, and whether they believe they themselves are capable of countering this threat. This perception of efficacy is very important, because people will usually not establish protecting behavior if they do not believe that this behavior is effective (Rogers, 1975).

In addition, with this efficacy appraisal, the PMT puts more emphasis on subjective appraisals that drive privacy protection (Dienlin & Metzger, 2016), whereas the communication privacy management theory and privacy calculus model focus on rational processes. This is an important difference, given the notion that people often do not or cannot calculate the risks and benefits rationally. The inability to protect oneself from a threat, such as a privacy threat, is assumed to induce irrational feelings such as helplessness and loss of control (Rogers, 1983), emphasizing the importance on less rational and more subjective factors that may explain protective behavior.

The PMT was originally developed to understand why people are motivated to protect themselves against health threats and to help identify the factors that may persuade a person to perform the appropriate, recommended behavior, ensuring people's safety or well-being. A growing number of studies have shown the relevance of the PMT to understand people's responses to privacy-related threats on the Internet, in contexts such as OBA (Ham, 2017), online shopping behavior (Milne et al., 2009), virus protection behavior (Lee, Larose, & Rifon, 2008), online information-sharing behavior (Chai et al., 2009; Marett, McNab, & Harris, 2011), and privacy protective behavior among adolescents (Youn, 2009).

The PMT posits that people's motivation to protect themselves from a specific threat depends on two things: a threat appraisal and a coping appraisal. The threat appraisal assesses the *perceived severity* of the threat and the *perceived susceptibility* to the threat. The coping appraisal assessed *self-efficacy* and *response efficacy*. Both appraisal processes influence people's motivation to protect themselves against a specific threat. Their relation is linear: When threat and coping efficacy are both perceived as high, people are motivated to protect themselves from the threat and adapt their behavior (Witte, 1992). Below, we will discuss how we expect these four factors to be related to protective behavior online.

Threat Appraisal

Whether people perceive a threat is first dependent on the perceived severity of the threat, which is defined as "an individual's belief about the seriousness of the threat" (Witte, 1992, p. 332). In this study, we investigate the perceived threat to people's online privacy. In the online environment, there is a threat to (informational) privacy when individuals do not have control over the collection and dissemination of personal information (Baruh et al., 2017; Nissenbaum, 2009). In essence, the threat to people's privacy online exists of companies collecting, using, and sharing personal data online. The fact that companies can perform these actions diminish people's control over their personal information.

Several studies have shown that the majority of people have concerns about their privacy online, and consider the targeting of adverting based on their personal information invasive and creepy (Boerman, Kruikemeier, & Zuiderveen Borgesius, 2017; Moore, Moore, Shanahan, & Mack, 2015; Ur, Leon, Cranor, Shay, & Wang, 2012). We, therefore, expect that most people will consider the collection, use, and sharing of personal data online as a serious problem. In addition, following the PMT, we expect that the more severe people think this threat to their online privacy is, the more likely they are to try to protect their privacy (Milne et al., 2009). Thus, we propose the following:

> **Hypothesis 1:** Higher levels of perceived severity of online privacy threat will lead to more protective behavior.

Second, the threat appraisal includes perceived susceptibility, which is "an individual's belief about his or her chance of experiencing the threat" (Witte, 1992, p. 332). According to the PMT, not only should a threat be perceived as serious but also people need to feel susceptible to the threat. When people do not feel that they are likely to actually face a threat, they will not be motivated to protect themselves, even when the threat itself is very serious.

In the context of online privacy, this means that even when people think that a threat to online privacy is a serious problem, they should also feel that this applies to them. Therefore, we conceptualize perceived susceptibility as the extent to which people think that their own personal information is collected, used, and shared by companies online. Following the PMT, perceived susceptibility to online privacy threats should positively influence protective behavior. Therefore, we pose the following hypothesis:

> **Hypothesis 2:** Higher levels of perceived susceptibility to online privacy threats will lead to more protective behavior.

Coping Appraisal

Next to the appraisal of the threat, the PMT suggests that people also evaluate the efficacy of their coping behavior. This process includes evaluations of self-efficacy and response efficacy. Self-efficacy is a person's belief of his or her own ability to perform the recommended response. In the context of online privacy, self-efficacy is defined as people's belief in their own ability to protect their privacy on the Internet (Ham, 2017; LaRose & Rifon, 2007; Rifon, LaRose, & Choi, 2005). Self-efficacy is related to behavior: People who believe in their capability to control their online privacy should also be more likely to engage in protective behavior than those with low self-efficacy (Bandura, 1978; LaRose & Rifon, 2007).

In line with this reasoning, prior studies showed that increased levels of individuals' self-efficacy led to more protective behavior (Milne et al., 2009), induced avoidance of OBA (Ham, 2017), and limited information sharing (Chai et al., 2009). In addition, people who actually have more Internet skills (Büchi et al., 2017), a better understanding of privacy tools and ad-blocking tools (Chanchary et al., 2018), and more digital literacy (Park, 2013) are more likely to protect their online privacy. Thus, we expect that people with high levels of self-efficacy perceive themselves as being able to cope with privacy risks and to, consequently, use more protective measures:

> **Hypothesis 3:** Higher levels of self-efficacy will lead to more protective behavior.

The coping appraisal also involves an evaluation of response efficacy, which is a person's belief of whether a response effectively prevents the threat (Witte, 1992). According to the PMT, people do have to believe that their response is effective to be motivated to engage in this behavior. Despite the growing literature adopting the PMT to online contexts, many did examine self-efficacy but very few also investigated the effect of response efficacy on protective behavior. In the context of virus protection, Lee et al. (2008) did find that belief in the effectiveness of virus protection measures increased the likelihood of adopting those measures to reduce or eliminate the harmful effects of an Internet virus. In line with these findings, and with the PMT, we, therefore, pose the following hypothesis:

> **Hypothesis 4:** Higher levels of perceived efficacy of protective behavior (i.e., response efficacy) will lead to more protective behavior.

Demographic Variables

Protective behavior has been shown to be related to demographic factors, such as education, gender, and age. Demographic variables are important as they provide insights into who are motivated and able to protect their privacy and who may need more help. The direction of these relationships, however, is not clear-cut.

People's level of education could have both a negative and a positive effect on protective behavior. On the one hand, research in the context of OBA found that the level of education has a negative effect on protective behavior (Smit et al., 2014). Smit et al. (2014) explain this by the notion that higher educated people also appear to have more knowledge about OBA and cookies, and having more knowledge, seems to be negatively related to having privacy concerns (Smit et al., 2014). In other words, people who know more about OBA and cookies appear to have fewer concerns and, thus, are less inclined to protect their privacy. On the other hand, having more knowledge and privacy literacy has also shown to increase privacy protection (e.g., Baruh et al., 2017; Ham, 2017; Park, 2013). Because an individual's level of education is likely related to his or her knowledge about privacy and protective behavior, we expect that education may influence privacy protective behavior.

Furthermore, based on the communication privacy management theory, there are some important differences between men and women in the context of privacy (Baruh et al., 2017). Women seem to be more concerned about their privacy online (Baruh et al., 2017; Moscardelli & Divine, 2007; Sheehan, 1999; Youn, 2009), and are more likely to apply protective behavior because they believe privacy is more important (Chai et al., 2009). However, other studies contradict these ideas, as some showed that men are more inclined to protect their online privacy (Milne et al., 2009; Smit et al., 2014), and that the actions that men take to protect their privacy differ from those used by women (Sheehan, 1999).

Age could also be an important factor explaining people's privacy concerns and protective behavior. However, the direction of the effect of age is unclear. Research into online privacy, in general, points out that there are no significant differences between younger and older adults with respect to privacy concerns and privacy protective behaviors (Hoofnagle, King, Li, & Turow, 2010). Research in the context of OBA showed that older people worry more about their privacy, are more negative about OBA, have less knowledge about OBA and cookies, and are more inclined to protect themselves than younger people (Smit et al., 2014). In the context of social media, however, research shows that younger adults have larger networks, disclose more about themselves for self-presentation purposes, and also are more likely to employ protective behaviors (e.g., deleting information to protect privacy; Kezer, Sevi, Cemalcilar, & Baruh, 2016; Van den Broeck, Poels, & Walrave, 2015).

To investigate and control for the effects of people's education, gender, and age, we ask a second research question:

> **Research Question 2:** Do people's (1) education, (2) gender, and (3) age influence privacy protective behavior?

Method

Sample

This study uses data from a questionnaire that was part of a larger longitudinal survey administered online by a large research institute in the Netherlands. The data used for this study were based on two waves; the data collection took place in April 2016 (Wave 1) and May 2017 (Wave 2). Data from this study were distributed among a representative sample. For the first wave, 1,523 respondents were invited to fill out the survey of whom 1,222 completed the survey (80%). For the second wave, 1,530 were invited, of whom 1,711 completed the survey (77%). In total, 928 respondents completed the relevant questions in both waves. This sample consisted of 49% female respondents, with a mean age in Wave 1 of 56 years (*SD* = 16.22 years, range = 18-89 years). Educational levels varied: 32.6% had finished lower education (no education or primary education), 32.5% medium levels of education (secondary education), and 34.9% higher education (bachelor's or master's degree).

Measures

All independent variables were measured in Wave 1. The dependent variable, people's protective behavior, was measured in both waves.

Perceived severity of online privacy threat. People's perceptions of the severity of the collection, usage, and sharing of their online behavior was measured by asking participants to what extent they agreed with the following statements (1 = *strongly disagree*, 7 = *strongly agree*): "Having companies collect my online behavior is a problem for me," "Having companies use my online behavior to show me advertisements is a problem for me," and "Having companies share my online behavior with other companies is a problem for me" (based on Ham, 2017). The mean of the three items is used as a measure of perceived severity (eigenvalue = 2.57, explained variance = 85.71; Cronbach's α = .92, *M* = 5.60, *SD* = 1.50).

Perceived susceptibility to online privacy threats. To measure people's perceived susceptibility to online privacy threats, we asked them to indicate to what extent they agreed with the following statements (1 = *strongly disagree*, 7 = *strongly agree*): "I believe that companies collect information about my online behavior," "I believe that companies use information about my online behavior to show me advertisements," and "I believe that companies share information about my online behavior with other companies" (based on Ngoh, Vishwanath, & Xu, 2015). We used the mean score of the three items as a scale of perceived susceptibility (eigenvalue = 2.48, explained variance = 82.75; Cronbach's α = .89, *M* = 5.71, *SD* = 1.39).

Self-efficacy. To measure people's perceived abilities on the Internet, we asked respondents to indicate the extent to which they agreed (or not; 1 = *strongly disagree*, 7 = *strongly agree*) with the following statements: "I am able to protect my personal information, such as my browsing 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" (based on LaRose & Rifon, 2007; Lee et al., 2008; Milne et al., 2009). The mean score of the three items is used as a scale of self-efficacy (eigenvalue = 2.20, explained variance = 73.99; Cronbach's α = .82, *M* = 3.22, *SD* = 1.44).

Response efficacy. To measure perceived response efficacy, we asked respondents to indicate (1 = *strongly disagree*, 7 = *strongly agree*, 9 = *do not know*) whether they believed the following protection behaviors would be an effective way to eliminate the collection, usage, and sharing of personal information on the Internet: (1) installing an ad blocker, (2) deleting cookies, (3) declining to accept cookies, (4) the usage of the private mode in a browser, (5) deleting browser history, (6) the usage of opt-out websites (such as www.youronlinechoices.com) to configure whether ads are based on personal online behavior, (7) activating the "Do Not Track" function in a browser, (8) the usage of special software in a browser (such as Ghostery and Abine Taco) that makes it harder for companies to collect personal information, and (9) filling out wrong information about yourself (such as a fake name or wrong email address) when asked for such information (based on Lee et al., 2008). All *do not know* responses were recoded as missing. Factor analysis revealed that the nine items loaded on one factor (eigenvalue = 5.90, explained variance = 65.57) and form a reliable scale (Cronbach's α = .93). Therefore, we used a mean score of the nine items as a measure of perceived response efficacy (*M* = 4.70, *SD* = 1.54). Because some answers were missing, the mean score could be calculated for 763 respondents.

Privacy protection behavior. We measured people's protective behavior by stating that there are various ways to protect one's personal information and privacy on the Internet. We then asked respondents how often (1) do you use an ad blocker, (2) delete cookies, (3) do you decide to refrain from visiting a website because it is only accessible when you accept cookies, (4) do you decline to accept cookies when website offers the choice, (5) do you use the private mode in your browser, (6) do you delete browser history, (7) do you use opt-out websites (such as www.youronlinechoices.com) to configure whether ads are based on personal data, (8) do you use the "Do Not Track" function in your browser, (9) do you use special software in your browser (such as Ghostery and Abine Taco) that makes it harder for companies to collect personal data, and (10) do you fill out wrong information about themselves (for instance, a fake name or wrong email address) when asked for such information. The 10 behaviors were based on prior studies measuring people's protective behavior online (e.g., Balebako et al., 2012; Büchi et al., 2017; McDonald & Cranor, 2010; Milne et al., 2009; Smit et al., 2014). Answer options were 1 = *never*, 2 = *rarely*, 3 = *occasionally*, 4 = *often*, 5 = *very often*, and 6 = *do not know*. All *do not know* responses were recoded as missing. Factor analysis revealed the 10 items loaded on one factor (Wave

1: eigenvalue = 3.67, explained variance = 36.74, factor loadings >.50; Wave 2: eigenvalue = 3.93, explained variance = 39.33, factor loadings >.55) and form a reliable scale (Cronbach's α Wave 1 = .80, Wave 2 = .82). We calculated a mean score of the 10 items as a scale of people's protective behavior ($M_{\text{Wave 1}} = 2.36$, $SD = 0.80$; $M_{\text{Wave 2}} = 2.44$, $SD = 0.85$). Because some answers were missing, the mean score could be calculated for 909 respondents in Wave 1 and 908 respondents in Wave 2.

Demographic variables. We also measured people's level of education (on a 6-point scale where 1 = *no or low educational level* and 6 = *high educational level*), gender (0 = *female*, 1 = *male*), and age (in years).

Results

Descriptive Statistics

Self-reported protective behavior. To answer Research Question 1, we report the descriptive statistics of people's self-reported protective behavior. The mean scores of the self-reported protective behavior suggest that, on average, people rarely to occasionally protect their online privacy ($M_{\text{Wave 1}} = 2.36$, $M_{\text{Wave 2}} = 2.44$). People did report to protect their online privacy more often in Wave 2 compared with Wave 1, $t(896) = -2.99$, $p = .003$.

To gain insights into people's specific behavior, Figure 1 present the descriptive statistics of all 10 protective behaviors in Wave 2 ($N = 928$), including the *do not know* option. The same descriptive statistics of Wave 1 can be found in the online appendix. Figure 1 shows that people most often delete cookies (71% occasionally to very often), delete their browser history (63% occasionally to very often), and decline cookies when given the opportunity (60% occasionally to very often) to protect their online privacy. More than half of the respondents (56%) also say they (occasionally to very often) refrain from visiting a website because it is only accessible when they accept cookies. Interestingly, 30% say they use ad blockers at least occasionally. The private mode (29%) and filling out wrong information (25%) are less commonly used. People least often use opt-out websites (8%), tracking prevention software (8%), or the Do Not Track function in their browser (12%).

The descriptive statistics also show that many people do not know what to answer to our questions, especially when they regard the private mode in their browser (34%), ad blockers (28%), Do Not Track (27%), opt-out websites (24%), and tracking prevention software (23%). This suggests that many people also have little knowledge about these ways of protective behavior.

Perceived threat and efficacy. On average, people perceive the collection, usage, and sharing of personal information online as a severe problem ($M = 5.60$, mode = 7) to which they are susceptible ($M = 5.71$, mode = 7). This means that perceived threat to online privacy is high.

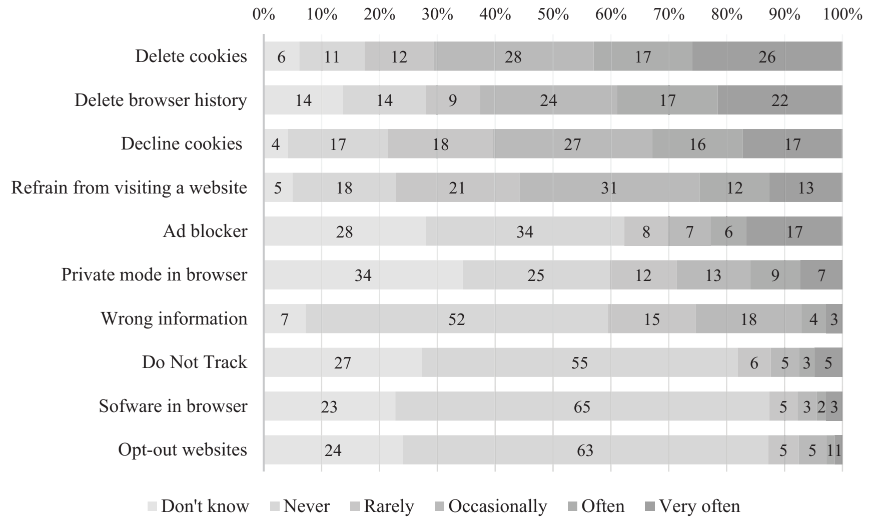

Figure 1. Descriptive statistics of online privacy protective behavior (Wave 2, *N* = 928).
Note. Numbers in bars are percentages. Protective behaviors are ordered from most often used to least often used.

Interestingly, people have far less confidence in their own efficacy to protect their personal information online (*M* = 3.22, mode = 4), but do believe that some responses can effectively limit the collection, usage, and sharing of personal information on the Internet (*M* = 4.70, mode = 7). When looking at the nine proposed behaviors separately, people think the most effective way to protect their online privacy is to delete cookies (*M* = 5.01), using the private mode in their browser (*M* = 4.90), and declining cookies (*M* = 4.85). These behaviors are followed by tracking prevention software (*M* = 4.76), removing browser history (*M* = 4.68), and Do Not Track (*M* = 4.68). People have least faith in filling out wrong information (*M* = 3.83), opt-out websites (*M* = 4.39), and ad blockers (*M* = 4.58). Thus, perceived efficacy seems to be mixed: People do seem to have confidence in the responses, but not in their own ability to effectively protect their online personal information.

Correlations

Table 1 shows the Pearson correlations between all variables. These results suggest that perceived severity, susceptibility, self-efficacy, and response efficacy are significantly related to protective behavior in both waves, and, thus, indicate at least cross-sectional relationships. In addition, the correlations between the four independent variables and control variables are nonsignificant or small in size (range = −.20-.21).

Table 1. Pearson Correlations Between Dependent and Independent Variables.

	1	2	3	4	5	6	7	8	9
1. Protective behavior W2	1								
2. Protective behavior W1	.63***	1							
3. Severity	.19***	.19***	1						
4. Susceptibility	.11**	.17***	.19***	1					
5. Self-efficacy	.13***	.16***	−.03	−.13***	1				
6. Response efficacy	.25***	.26***	.05	.16***	.17***	1			
7. Education	.03	.00	−.07*	.21***	−.15***	.08*	1		
8. Gender	−.01	−.07*	.08*	−.08*	−.05	−.05	−.11**	1	
9. Age	−.07*	−.06	.12***	−.14***	−.05	−.07	−.20***	−.09**	1

Note. W2 = Wave 2; W1 = Wave 1.
*p < .05. **p < .01. ***p < .001.

Model Testing

To test the hypotheses, we deployed a “lagged dependent variable regression” model, what has also been called the “conditional change” model (Finkel, 1995), in which we included self-reported protective behavior measured in the second wave as the dependent variable. The strength of this model is that it controls for prior privacy protection behaviors (this is the lagged value of the dependent variable) in Wave 1. So, when this lagged dependent variable is present, we can analyze *changes* in the dependent variable over time.

We ran three separate models: (1) the effect of only previous privacy protective behavior, (2) the effect of previous behavior and the PMT factors, and (3) the effects of previous behavior, the PMT factors, and the demographic variables. Table 2 presents the results of the analyses. The first model showed that previous privacy protective behavior in Wave 1 (April 2016) significantly predicts change in privacy protective behavior in Wave 2 (May 2017; adjusted $R^2 = .41$). Adding the PMT factors to this model increases the R^2 significantly by .01 (p F change < .001) to $R^2 = .42$. This confirms the idea that the PMT factors do explain some of the change in privacy protective behavior. Finally, the third model showed that adding the demographic variables does not significantly change the R^2 (p F change = .564), showing that education, gender, and age do not predict change in privacy protective behavior.

More specifically, the results revealed that perceived severity ($B = 0.05$, $SE = 0.02$, $\beta = 0.09$, $p = .004$) and response efficacy ($B = 0.05$, $SE = 0.02$, $\beta = 0.09$, $p = .001$) both have a significant small positive effect on people’s protective behavior. In other words, the more serious people perceive the collection, usage, and sharing of their personal information on the Internet, the more likely they are to protect their privacy online. In addition, the more people think that the protective behaviors are effective,

Table 2. Lagged Dependent Variable Regressions Predicting Change in Online Privacy Protective Behavior (Wave 2).

	Model 1			Model 2			Model 3		
	B (*SE*)	β	*p*	*B* (*SE*)	β	*p*	*B* (*SE*)	β	*p*
Constant	0.88 (0.07)		.000	0.52 (0.16)		.001	0.45 (0.21)		.034
Protective behavior Wave 1	0.66 (0.03)	0.64	.000	0.61 (0.03)	0.59	.000	0.62 (0.03)	0.59	.000
Perceived severity				0.05 (0.02)	0.08	.005	0.05 (0.02)	0.09	.004
Perceived susceptibility				−0.02 (0.02)	−0.03	.381	−0.02 (0.02)	−0.03	.272
Self-efficacy				0.02 (0.02)	0.04	.164	0.03 (0.02)	0.05	.117
Response efficacy				0.05 (0.02)	0.10	.001	0.05 (0.02)	0.09	.001
Education							0.02 (0.02)	0.04	.180
Gender							0.01 (0.05)	0.01	.775
Age							0.00 (0.00)	−0.01	.831
	$F(1, 757) = 518.43$, $p < .001$ Adjusted $R^2 = .41$			$F(5, 753) = 110.52$, $p < .001$ Adjusted $R^2 = .42$			$F(8, 750) = 69.24$, $p < .001$ Adjusted $R^2 = .42$		

Note. Gender is coded 0 = female, 1 = male. *B* = unstandardized regression coefficient; *SE* = standard error associated with the *b* coefficient; β = standardized regression coefficient.

the more likely they are to actually use them. This means that Hypotheses 1 and 4 are supported.

Surprisingly, perceived susceptibility ($p = .272$) and self-efficacy ($p = .117$) do not appear to significantly influence people's protective behavior. This means Hypotheses 2 and 3 are not supported. Furthermore, answering Research Question 2, education ($p = .180$), gender ($p = .775$), and age ($p = .831$) do not significantly affect protective behavior when we use a longitudinal data approach.

Model Robustness Checks

We conducted several robustness checks. First, we reran the analysis with 10,000 bootstrap samples, which led to the same results. Furthermore, respondents had the opportunity to answer *do not know* to the questions about their protective behavior. In the reported analyses, all *do not know* responses were coded as missing. To test the robustness of the model, we also created protective behavior measures in which we recoded the *do not know* responses into *never*. As this increased the number of respondents scoring 1 (*never*), this lowered the means of the protective behavior variables ($M_{\text{Wave 1}} = 2.11$, $SD = 0.72$; $M_{\text{Wave 2}} = 2.19$, $SD = 0.75$). The results revealed similar outcomes, with a higher explained variance (adjusted $R^2 = .47$). The difference with the initial model was that self-efficacy ($B = 0.03$, $SE = 0.02$, $\beta = 0.05$, $p = .091$) and education ($B = 0.03$, $SE = 0.01$, $\beta = 0.05$, $p = .061$) appeared to be marginally significant predictors of protective behavior.

Moreover, to gain insights into who said *do not know* and why education seemed to play a role, we created 10 dummy variables for the separate protective behaviors with 1 = *do not know* and 0 = *all other answers*. We then ran 10 logistic regressions with the new *do not know* variables as dependent variables and education as predictor. These analyses revealed that higher levels of education significantly (all ps $< .042$) reduce the chance that people say *do not know* for nine out of 10 behaviors (private mode in browser, $p = .688$). This suggests that mostly people with lower levels of education say that they do not know whether they perform the different protective behaviors, which indicates that less educated citizens are less likely to be familiar with these modes of self-protection.

Finally, to examine the relationship between the variables in both causal directions, we also ran a cross-lagged panel model. However, a full cross-lagged model was not possible as one variable (i.e., self-efficacy) was unfortunately not measured in our second wave. Yet, because all the other variables were measured in both waves, we could still assess the relationship between the other three variables (i.e., severity, susceptibility, and response efficacy) and protection behavior in both causal directions. This is also justifiable, as the missing variable was not significantly predicting behavior in Wave 2 in our conditional change model (but we still include this in the cross-lagged panel model). The results from our cross-lagged panel model confirmed our initial analyses (in which the *do not know* answers were recoded as *never*). The results show that severity and response efficacy in Wave 1 influence privacy protection behavior in Wave 2. Thus, these results verify our findings from the initial analyses. Interestingly, the results of the cross-lagged model also revealed a reciprocal influence; we found that privacy protection behavior in Wave 1 positively affected response efficacy in Wave 2.

Discussion

In the context of rising privacy concerns on the Internet, in this study, we examined (1) whether people protect their online privacy, (2) which methods they use most often, and (3) what factors of the PMT may explain protective behavior. Our large-scale panel study reveals insights to the three subjects. First, we find that, on average, people rarely to occasionally protect their online privacy. People's self-reported protective behavior did increase slightly between April 2016 and May 2017. These findings not only confirm prior studies that have suggested that people generally do try to protect their privacy online (e.g., Büchi et al., 2017; McDonald & Cranor, 2010; Smit et al., 2014) but also indicate that many people could do a lot more to protect their privacy online.

Second, our study finds large differences between the measures people take to protect their online privacy. More than 60% of the people delete cookies, decline cookies when given the opportunity, or delete their browser history at least occasionally to protect their online privacy. People least often use opt-out websites, tracking prevention software, and the Do Not Track function in their browser. Ad blockers appear to be used at least occasionally by 30% of the respondents. Interestingly, many people did not know how to answer our questions. More than 20% did not know whether they used tracking prevention software, opt-out websites, Do Not Track, ad blockers, or the private mode in their browser. This suggests that many people have little knowledge about these ways of protective behavior.

Third, we find that two of the four factors of the PMT have significant small positive effects on changes in protective behavior (i.e., perceived severity and response efficacy). Overall, our study demonstrated that the threat appraisal is high: People perceive the collection, usage, and sharing of personal information online as a severe problem to which they are susceptible. Moreover, perceived severity significantly and positively predicted protective behavior. In line with the PMT and prior studies (Milne et al., 2009), the more severe people think this threat to their online privacy is, the more likely they are to try to protect their privacy. The lack of evidence of such an effect of the perceived susceptibility may be explained by the low variance in this construct: 79% of the people scored 5 or higher. As almost all people believe that their personal information is being collected, used, and shared by companies online, there may be a ceiling effect.

Our findings with regard to the coping appraisal are mixed: People seem to have little confidence in their own efficacy to protect their personal information online, but do believe that some responses can effectively eliminate the collection, usage, and sharing of personal information on the Internet. The low levels of self-efficacy correspond to earlier findings that people have limited knowledge about cookies (Smit et al., 2014), do not know why they manage cookies (McDonald & Cranor, 2010), and do not understand all the tools that are available (Leon et al., 2012). This lack of knowledge seems to be reflected in people's own perceptions of their ability to secure their online privacy. Despite the low self-confidence, people do seem to have some confidence in the actual options they have, as the average perceived efficacy of the nine behaviors range between 3.83 and 5.01. In addition, when testing the PMT, the perceived response efficacy significantly predicts protective behavior, whereas we did not find evidence for such an effect of self-efficacy. This suggests that it is not people's own efficacy that can encourage privacy protection, but their trust in the effectiveness of taking measures that influences their behavior.

Prior studies have indicated a lack of accurate knowledge of tracking prevention tools (Chanchary et al., 2018) and people find many existing tools too difficult to use and to configure (Leon et al., 2012; Shirazi & Volkamer, 2014). Moreover, few, if any, tools protect against all tracking technologies, and the effectiveness of tools often depends on the configuration (Acar et al., 2014; Bujlow, Carela-Español, Solé-Pareta, & Barlet-Ros, 2017; Estrada-Jiménez et al., 2017). With that caveat, we give a rough indication of which tools and tactics can be effective to protect one's privacy and to limit online tracking.

Our study indicates that deleting cookies is the most used privacy protective measure, and people also believe this is most effective. Indeed, deleting cookies helps to limit online data collection through tracking. But deleting cookies does not help against *all* types of online tracking. Apart from cookies, companies use many other tracking techniques, such as flash cookies and device fingerprinting (Hoofnagle, Soltani, Good, Wambach, & Ayenson, 2012). Nevertheless, deleting cookies from one's browser does limit online tracking, as cookies are still a popular tracking method (Estrada-Jiménez et al., 2017). In sum, people's trust in the effectiveness of deleting cookies is not entirely justified. People also indicated to have quite some trust in the effectiveness of declining cookies. However, declining cookies and also refraining from visiting websites that drop cookies are not very effective to protect one's privacy. These measures only work when a site asks consent for dropping (tracking) cookies, but many sites drop such cookies surreptitiously.

People also indicated to trust the private mode in their browsers. However, whether using a browser's private mode limits online tracking depends on the browser type. Most browsers, but not all, limit (but do not stop) tracking when set to "private" (Bujlow et al., 2017; Tsalis, Mylonas, Nisioti, Gritzalis, & Katos, 2017).

Interestingly, people have very little faith in ad blockers, but running an ad blocker (usually a plug-in for one's browser) can be an effective way to limit online tracking, if configured correctly. Many ad blockers do not load any advertising, and thereby limit online tracking (Gervais, Filios, Lenders, & Capkun, 2017; Wills & Uzunoglu, 2016). Using tracking prevention software (such as Privacy Badger and Ghostery) can also be effective to limit tracking (Balebako et al., 2012; Gervais et al., 2017; Merzdovnik et al., 2017; Wills & Uzunoglu, 2016). However, many people find such ad blockers and tracking prevention software confusing, and may choose the wrong (default) settings, while they think they protect themselves (Cranor, 2012; Leon et al., 2012).

Deleting one's browser history primarily protects people from other users of the same browser seeing their browsing history, and is less effective to protect oneself against online data collection. However, deleting browser history including the browser cache, could help to protect against some tracking methods (Bujlow et al., 2017). In some browsers (such as Firefox), users can manage their cookies under the heading "history." Perhaps, some people delete their browsing history to delete cookies.

Giving wrong information, such as a fake email address, can reduce the amount of spam one receives, but does generally not help against online tracking. Opt-out websites, such as www.youronlinechoices.com, generally do not block tracking and data collection, but only limit targeted advertising (Balebako et al., 2012). Hence, opt-out sites are not effective as a privacy protection measure. Setting the browser's Do Not Track function is, at present, not effective in limiting online tracking either. Most tracking companies do not react to Do Not Track signals (Balebako et al., 2012; Bujlow et al., 2017). Do Not Track could become an effective measure in the future, for instance, if lawmakers required companies to respect Do Not Track signals (Zuiderveen Borgesius, van Hoboken, Fahy, Irion, & Rozendaal, 2017).

Furthermore, unlike prior research, age, and gender do not seem to predict protective behavior. Although prior studies have shown that women are more concerned about their privacy online (Baruh et al., 2017; Moscardelli & Divine, 2007; Sheehan, 1999; Youn, 2009), the effects of gender on protective behavior are inconclusive. Our study does not provide evidence for different protective behaviors between men and women. In addition, although prior studies found that older people are more inclined to protect themselves against OBA than younger people (Smit et al., 2014), we do not find evidence for an effect of age on general protective behavior. Our study did suggest that education does play a role. We found that mostly people with lower education levels say that they do not know whether they perform the different protective behaviors. This means that less educated citizens are less likely to be familiar with the measures they can take to protect their online privacy, and this results in less protective behavior. This replicates the findings of Smit et al. (2014), who found that people's level of education negatively affects protective behavior.

One important limitation of our study is the fact that we measured protective behavior with self-reports. The self-reported measure may have led to overreporting of protective behavior due to memory and/or social desirability issues (Baruh et al., 2017). However, as a meta-analysis did not find evidence of differences between behavioral intentions and behaviors in terms of utilization of privacy protective measures (Baruh et al., 2017), we believe that self-reported measures can provide important insights.

Furthermore, we asked respondents about 10 different behaviors based on the literature (e.g., Balebako et al., 2012; Büchi et al., 2017; McDonald & Cranor, 2010; Milne et al., 2009; Smit et al., 2014) and aimed to include as many behaviors that can mitigate the collection, usage, and sharing of personal information to protect their online privacy. However, this list is not exhaustive. Due to limited space and time in our survey, there are several behaviors that we did not include, such as using a virtual private network, only reading email in plain text, and deleting Adobe Flash from one's computer. Future research could include an even broader variety of protective behaviors.

A third limitation of our study is the conceptualization of the threat to privacy online. Based on the idea that privacy considers the control over personal information, we conceptualized the threat to privacy online as those actions that can limit this control (i.e., the collection, usage, and sharing of personal information). With this operationalization, we focused on the primary threat to people's privacy. However, one can also define the threat as the negative consequences that data collection, usage, and sharing may have, such as data privacy, data breaches, identity theft, and discrimination. By choosing to focus on the primary issue of data collection, and not on the possible negative consequences, this may have caused the high scores in perceived susceptibility. Our study shows that people are well aware of the collection, usage, and sharing of their personal information online. However, our study does not show whether they think they are susceptible to possible negative consequences of these actions. Future research into people's perception of threat (i.e., severity and susceptibility) could combine both the primary threat (i.e., data collection, usage, and sharing) and possible negative consequences of these actions that also cause a threat to privacy online.

Notwithstanding the limitations, this study has some important theoretical implications. Although some studies into online privacy protection relied on privacy management theory (Baruh et al., 2017; Petronio, 2002) and privacy calculus model (e.g., Dienlin & Metzger, 2016; Krasnova et al., 2010), many of the studies into online privacy protection behavior lacked a theoretical foundation. In this study, we aimed to change this by using the PMT to understand which factors may explain privacy protective behavior. Although the PMT was originally developed to understand people's motivation to protect themselves against health threats, a growing number of studies have applied the PMT to privacy-related threats on the Internet (e.g., Chai et al., 2009; Ham, 2017; Youn, 2009). The theory proved to be a valuable way to understand why people protect their online privacy, as two of the four factors significantly influence people's behavior: perceived severity and response efficacy.

Drawing on the PMT, our study also provides practical insights into what should be communicated to encourage protective behavior. On average, people rarely to occasionally protect their online privacy. In addition, the perceived threat is high, indicating that people are aware of the threat to their online privacy. However, many people do not know what to answer in questions about highly effective behaviors (e.g., ad blockers)—which is an indication for little knowledge. Thus, we believe that there is much to gain as people could do a lot more to protect their privacy online. When governments or consumer organizations wish to motivate people to protect their online privacy, these nudges and messages should address the perceived severity and response efficacy as these two factors have significant positive effects on protective behavior. People could be educated about the severity of the threat by explaining to them how the collection, usage, and sharing of your personal data online could be a threat to one's privacy. In addition, response efficacy could be addressed with messages that introduce people to protective behaviors and show how these can effectively prevent tracking and improve your privacy. In our study, self-efficacy did not significantly increase protective behavior. This suggests that even people with low confidence (i.e., low perceived self-efficacy) can be motivated to protect behavior, as long as they are presented with methods that are perceived as effective.

Next to theoretical and practical implications, our study also has important implications for policy makers. Our findings indicate that consumers are not empowered: People have little confidence in their abilities to protect their own privacy. Moreover, several popular tactics, such as declining cookies, are not very effective to limit online tracking and to protect privacy. People rarely use tools that can limit online tracking and protect privacy (such as ad blockers and tracking prevention software). These results have several implications. First, if policy makers want people to enjoy privacy, they must protect privacy through regulation. The EU just updated its privacy legislation (EU General Data Protection Regulation, 2016), and aims to adopt new rules specifically for online tracking and privacy (European Commission, 2017). It remains to be seen whether these laws will be effective in protecting privacy. Second, researchers showed that OBA is possible without large-scale data collection (Estrada-Jiménez et al., 2017; Toubiana, Narayanan, Boneh, Nissenbaum, & Barocas, 2010), but such technologies are not widely used yet. Policy makers could, through regulation, push companies toward using such methods. Third, there is a need for education and awareness building. Although some tools exist that can help people to protect themselves against online data collection, few people use them. Finally, easy-to-use privacy protection tools should be developed; policy makers could help by funding research.

Acknowledgments

The authors would like to thank Rob van Eijk and Ward van Zoonen for their valuable suggestions.

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: The research was funded by and made possible through the University of Amsterdam Research Priority Area "Personalised Communication" (personalized-communication.net), principal investigators Natali Helberger and Claes de Vreese.

ORCID iD

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

Supplemental Material

Supplemental material for this article is available online.

References

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 674-689). doi:10.1145/2660267.2660347

Balebako, R., Leon, P. G., Shay, R., Ur, B., Wang, Y., & Cranor, L. F. (2012). *Measuring the effectiveness of privacy tools for limiting behavioral advertising* (Web 2.0 Security and Privacy Workshop). Retrieved from http://www.andrew.cmu.edu/user/pgl/w2sp2012.pdf

Bandura, A. (1978). Self-efficacy: Toward a unifying theory of behavioral change. *Advances in Behaviour Research and Therapy*, *1*, 139-161. doi:10.1016/0146-6402(78)90002-4

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*, 579-596. doi:10.1177/1461444815614001

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

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, *46*, 363-376. doi:10.1080/00913367.2017.1339368

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the Association for Information Science and Technology*, *58*, 157-165. doi:10.1002/asi.20459

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. doi: 10.1080/1369118X.2016.1229001

Bujlow, T., Carela-Español, V., Solé-Pareta, J., & Barlet-Ros, P. (2017). A survey on web tracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE*, *105*, 1476-1510. doi:10.1109/JPROC.2016.2637878

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

Chanchary, F., Abdelaziz, Y., & Chiasson, S. (2018). Privacy concerns amidst OBA and the need for alternative models. *IEEE Internet Computing*, *22*, 52-61. doi:10.1109/MIC.2017.3301625

Chen, H., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*, 13-19. doi:10.1089/cyber.2014.0456

Cranor, L. F. (2012). Can users control online behavioral advertising effectively? *IEEE Security & Privacy*, *10*, 93-96. doi:10.1109/MSP.2012.32

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*, 368-383. doi: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*, 285-297. doi:10.1002/ejsp.2049

Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., & Forné, J. (2017). Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, *100*, 32-51. doi:10.1016/j.comcom.2016.12.016

EU ePrivacy Directive. (2009). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:02002L0058-20091219

EU General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General data protection regulation). *Official Journal of the European Union*, *119*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

European Commission. (2017). *Proposal for a regulation of the European parliament and of the council, concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/EC (Regulation on privacy and electronic communications)*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

Federal Trade Commission. (2012). *Protecting consumer privacy in an era of rapid change*. Retrieved from www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior*, *33*, 153-162. doi:10.1016/j.chb.2014.01.009

Finkel, S. E. (1995). *Causal analysis with panel data*. Thousand Oaks, CA: SAGE.

Gervais, A., Filios, A., Lenders, V., & Capkun, S. (2017). Quantifying web adblocker privacy. In *European Symposium on Research in Computer Security* (pp. 21-42). doi:10.1007/978-3-319-66399-9_2

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

Gomez, J., Pinnick, T., & Soltani, A. (2009). *KnowPrivacy*. Retrieved from http://escholarship.org/uc/item/9ss1m46b

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

Ham, C., & 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. doi:10.1016/j.chb.2016.03.076

Hargittai, E., & Hinnant, A. (2008). Digital inequality: Differences in young adults' use of the internet. *Communication Research*, *35*, 602-621. doi:10.1177/0093650208321782

Helsloot, L. J., Tillem, G., & Erkin, Z. (2017). *Privacy concerns and protection measures in online behavioural advertising*. Retrieved from https://pdfs.semanticscholar.org/29ba/07c3587169e158467b43e3ff6cefaa3b932c.pdf

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies?* (Research report). Retrieved from http://ssrn.com/abstract=1589864

Hoofnagle, C. J., Soltani, A., Good, N., Wambach, D. J., & Ayenson, M. D. (2012). *Behavioral advertising: The offer you cannot refuse*. Retrieved from https://ssrn.com/abstract=2137601

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), Article 2. doi:10.5817/CP2016-1-2

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

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, *41*, 127-149. doi:10.1111/j.1745-6606.2006.00071.x

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, *27*, 445-454. doi:10.1080/01449290600879344

Leon, P. G., Ur, B., Shay, R., Wang, Y., Balebako, R., & Cranor, L. F. (2012). Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp 589-598). doi:10.1145/2207676.2207759

Malandrino, D., Scarano, V., & Spinelli, R. (2013). How increased awareness can impact attitudes and behaviors toward online privacy protection. In 2013 International Conference on Social Computing (pp. 57-62). doi:10.1109/SocialCom.2013.15

Marett, K., McNab, A. L., & Harris, R. B. (2011). Social networking websites and posting personal information: An evaluation of protection motivation theory. *AIS Transactions on Human-Computer Interaction*, *3*, 170-188. Retrieved form http://aisel.aisnet.org/thci/vol3/iss3/2

McDonald, A. M., & Cranor, L. F. (2010). *Beliefs and behaviors: Internet users' understanding of behavioral advertising* (TPRC 2010). Retrieved from http://aleecia.com/authors-drafts/tprc-behav-AV.pdf

Merzdovnik, G., Huber, M., Buhov, D., Nikiforakis, N., Neuner, S., Schmiedecker, M., & Weippl, E. (2017). Block me if you can: A large-scale study of tracker-blocking tools. The Institute of Electrical and Electronics Engineers, Inc. (Ed.), In *Proceedings of the 2nd IEEE European Symposium on Security and Privacy,* Paris, France. Retrieved from https://www.researchgate.net/

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, *12*, 335-361. doi:10.1111/j.1083-6101.2007.00328.x

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*, 449-473. doi:10.1111/j.1745-6606.2009.01148.x

Moore, R. S., Moore, M. L., Shanahan, K. J., & Mack, B. (2015). Creepy marketing: Three dimensions of perceived excessive online privacy violation. *Marketing Management Journal*, *25*, 42-53.

Moscardelli, D. M., & Divine, R. (2007). Adolescents' concern for privacy when using the internet: An empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family and Consumer Sciences Research Journal*, *35*, 232-252. doi:10.1177/1077727X06296622

Ngoh, Z., Vishwanath, A., & Xu, W. (2015). *Predicting privacy protection behavior on social networking sites: An integrated framework of protection motivation and uses and gratifications*. Presented at the Annual Conference of the International Communication Association, San Juan, Puerto Rico.

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

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

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.

Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, *39*, 339-362. doi:10.1111/j.1745-6606.2005.00018.x

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*, 93-114. doi: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 and R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153-176). New York: Guilford Press.

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, *13*(4), 24-38. doi:10.1002/(SICI)1520-6653(199923)13:4<24::AID-DIR3>3.0.CO;2-O

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising*, *28*, 37-51. doi:10.1080/00913367.1999.10673588

Shirazi, F., & Volkamer, M. (2014). What deters Jane from preventing identification and tracking on the web? In Proceedings of the 13th Workshop on Privacy in the Electronic Society (pp. 107-116). doi:10.1145/2665943.2665963

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. doi:10.1016/j.chb.2013.11.008

Toubiana, V., Narayanan, A., Boneh, D., Nissenbaum, H., & Barocas, S. (2010). *Adnostic: Privacy preserving targeted advertising*. Retrieved from http://www.nyu.edu/pages/projects/nissenbaum/papers/adnostic.pdf

Tsalis, N., Mylonas, A., Nisioti, A., Gritzalis, D., & Katos, V. (2017). Exploring the protection of private browsing in desktop browsers. *Computers & Security*, *67*, 181-197. doi:10.1016/j.cose.2017.03.006

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). *Americans reject tailored advertising and three activities that enable it*. doi:10.2139/ssrn.1478214.

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In Proceedings of the Eighth Symposium on Usable Privacy and Security (Article 4). doi:10.1145/2335356.2335362

Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*, *1*(2). doi:10.1177/2056305115616149

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *6*(1), Article 3. doi:10.5817/CP2012-1-3

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Wills, C. E., & Uzunoglu, D. C. (2016). What ad blockers are (and are not) doing. In 2016 Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (pp. 72-77). doi:10.1109/HotWeb.2016.21

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

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*, 389-418. doi:10.1111/j.1745-6606.2009.01146.x

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology & Behavior*, *11*, 763-765. doi:10.1089/cpb.2007.0240

Zuiderveen Borgesius, F. J. (2015). Behavioural sciences and the regulation of privacy on the internet. In A. Sibony, & A. Alemanno (Eds.), *Nudging and the law - what can EU law learn from behavioural sciences?* (pp. 179-207). Portland, Oregon: Hart Publishing.

Zuiderveen Borgesius, F. J., van Hoboken, J., Fahy, R. P., Irion, K., & Rozendaal, M. (2017). *An assessment of the commission's proposal on privacy and electronic communications*. European Parliament.

Author Biographies

Sophie C. Boerman (PhD, University of Amsterdam, 2014) is an assistant professor of persuasive communication at the Amsterdam School of Communication Research (ASCoR) at the University van Amsterdam. She is also a member of the board of the European Advertising Academy (EAA). Her research mainly focuses on the persuasive effects of embedded and personalized advertising, and how informing consumers about advertising may influence the use of persuasion knowledge and its persuasive outcomes.

Sanne Kruikemeier (PhD, University of Amsterdam, 2014) is an assistant professor of political communication at the ASCoR at the University van Amsterdam. Her research mainly focuses on the content and effects of online communication in a political context. She is currently cochair of the political communication division of the Netherlands-Flanders Communication Association (NEFCA).

Frederik J. Zuiderveen Borgesius (PhD, University of Amsterdam, 2014) is a researcher at the Institute for Information Law (IViR) at the University of Amsterdam. His research mostly focuses on privacy, discrimination, and the law in the context of new technologies.