MUNI FSS

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Segijn, C. M., Opree, S. J., & van Ooijen, I. (2022). The Validation of the Perceived Surveillance Scale. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16*(3), Article 9. https://doi.org/10.5817/CP2022-3-9

The Validation of the Perceived Surveillance Scale

Claire M. Segijn[1], Suzanna J. Opree[2], & Iris van Ooijen[3]

[1] Hubbard School of Journalism & Mass Communication, University of Minnesota, USA
[2] Erasmus School of History, Culture and Communication ESHCC, Erasmus University Rotterdam, Netherlands
[3] Behavioral Science Institute, Radboud University, Netherlands

Abstract

Data-driven practices, such as personalized communication, computational advertising, and algorithmic decision making, are now commonplace. However, they have been criticized for (mis)uses of personal data and invasions of people's privacy. Recently, scholars have started to examine the concept of perceived surveillance to obtain more insight into the perceptions and effectiveness of data-driven communication. Despite the growing research interest in perceived surveillance, there is no validated scale to measure this concept. This study aimed to validate the Perceived Surveillance Scale. The reliability and validity of the scale were tested in two surveys (N = 137 and N = 1,008) and one experiment (N = 527). In all three studies, the scale showed good reliability. Regarding construct validity, the results showed that, as expected, the Perceived Surveillance Scale was positively related to privacy concerns, privacy risk perception, perceived vulnerability, perceived severity, creepiness, surveillance concerns, and perceived personalization. In line with the predictions, the scale was negatively related to personalization attitudes. The Perceived Surveillance Scale can assess differences in perceptions of or responses to data-driven communication in different communication domains.

Keywords: perceived surveillance; privacy; scale validation; data-driven communication; personalized communication; algorithmic decision making

Editorial Record

First submission received:
May 18, 2021

Revisions received:
April 6, 2022
May 17, 2022
June 9, 2022

Accepted for publication:
June 13, 2022

Editor in charge:
Lenka Dedkova

Introduction

In today's society, communication is driven by data. Enhanced computer capabilities, the development of mathematical models and algorithms, and the presence of technology infrastructure makes it possible to optimize message effectiveness by personalizing communication to the recipients' interests, (online) behaviors, and needs (Hudders et al., 2019; Huh & Malthouse, 2020; Yun et al., 2020). Although these practices have been thought to increase message effectiveness compared to mass communication because of their increased relevance to the recipient (De Keyzer et al., 2015; Zhu & Chang, 2016), they have also been criticized for (mis)using personal data and invasions of privacy (Awad & Krishnan, 2006; Lee et al., 2011; Turow et al., 2009). For example, people report that these data collection practices give them the feeling of being watched (Phelan et al., 2016). Such feelings are further enhanced by the increasing availability of people's online and offline data, which facilitates the use of these data as input for messages (Duffy & Chan, 2019). Additionally, due to negative media messages about personalization practices, such as data breaches, people are slowly becoming more aware of data collection practices in online environments (i.e., gaining knowledge about data collection practices), which may also

contribute to perceptions of surveillance (Byers, 2018). Moreover, these perceptions of surveillance could lead to more resistance to the message (Farman et al., 2020; Segijn et al., 2021) and could also affect people's media use, such as using less media, using media differently, or consuming different media content (Büchi et al., 2020; McDonald & Cranor, 2010; Stiff, 2019; Strycharz et al., 2022).

Recently, scholars have started examining the concept of *perceived surveillance* (e.g., Farman et al., 2020; Segijn & van Ooijen, 2020; Segijn et al., 2021; Sifaoui et al., 2022) to obtain more insight into the perceptions of and responses to data-driven practices. Surveillance is defined as "the watching, listening to, or recording of an individual's activities" (Solove, 2006, p. 490). The perception of being watched is defined as *perceived* surveillance (Farman et al., 2020; Segijn & van Ooijen, 2020), which does not necessarily have to correspond with actual surveillance because either people do not have perceptions of surveillance while they are being surveilled or vice versa. An example is the perception people may have that a smart device is listening in to their conversations (Frick et al., 2021). Despite the growing research interest in the concept of perceived surveillance, there is no validated scale to measure the concept. Therefore, the aim of the current study was to validate the existing Perceived Surveillance Scale that has been used in previous research (e.g., Segijn & van Ooijen, 2020; Segijn et al., 2021; Sifaoui et al., 2022).

Strengths and Contributions

The current study has at least three strengths. First, we conducted three consecutive studies to validate the scale. This allowed us to test the reliability and to validate the factorial structure of the scale across different scenarios and different populations, which increases the applicability of the scale. Additionally, validating the scale using a general sample enables researchers to further examine individual differences, such as the notion that older generations have different perceptions related to privacy and surveillance (Kezer et al., 2016; Segijn & van Ooijen, 2020) or to study how different personality traits (e.g., Big Five)—which have been studied in the context of personalization (Winter et al., 2021; Zarouali et al., 2020)—relate to perceived surveillance. Second, we tested to what extent the Perceived Surveillance Scale assesses people's *perceptions of* different situations (e.g., personalization techniques) as well as people's *responses to* a certain situation (e.g., exposure to personalized communication scenario). The former might be more applicable to survey research, while the latter might be more applicable to experimental research, both common methods to study data-driven communication. Finally, we tested the scale's relationship with other relevant concepts that are often measured in the context of data-driven communication to test the scale's convergent validity.

The Perceived Surveillance Scale can be used to study the perceptions of and responses to data-driven communication in different research domains. Such data-driven domains include political microtargeting (e.g., Feezell et al., 2021; Kruikemeier et al., 2016), personalized advertising (e.g., Baek & Morimoto, 2012; Kim & Huh, 2017; Maslowska et al., 2016), and tailored health messages (e.g., Bol et al., 2018, 2020). For example, personalized communication has both benefits and costs (Awad & Krishnan, 2006; Dinev & Hart, 2006). Whereas benefits include the advantages that are associated with data disclosure (e.g., the ability to use online services), costs may comprise risk beliefs or privacy concerns that are associated with personal data disclosure (Dinev & Hart, 2006) or ethical side effects such as self-censorship due to surveillance (Büchi et al., 2020, 2022).

As surveillance will become a more prominent phenomenon in today's digital world (Christl, 2017), the Perceived Surveillance Scale may provide a much needed instrument that enables researchers to test perceived surveillance as one of the costs of (or threats associated with) personalized communications. Rather than measuring positive or negative associations with privacy concerns (e.g., privacy concerns, creepiness), or measuring awareness of the consequences of surveillance (e.g., awareness of personalization, perceived risk), the Perceived Surveillance Scale encapsulates merely the perception of the phenomenon of digital surveillance, a phenomenon that takes place mostly invisibly and its subjective perception may therefore differ greatly across individuals and situations. As we believe that this specific perception of being watched may be associated with negative psychological consequences for individuals, we believe that the concept of perceived surveillance is an important variable that drives responses to personalized communication. Moreover, the scale could also be used outside the personalized communication domain to measure perceptions of and response to other data driven technologies, such as smart devices (Frick et al., 2021), computational advertising (Huh & Malthouse, 2020), and algorithmic decision making (Zarouali et al., 2021).

Additionally, previous research has found that the perception of personalized messages could carry over to the message's effectiveness (Acquisti et al., 2006; Aguirre et al., 2015). Therefore, developing a validated scale of

perceived surveillance will also provide more insights for practitioners about the effectiveness of personalized messages that are used. Furthermore, the concept of perceived surveillance could contribute to privacy debates related to personalized communication that needs to be held both in society and among practitioners (Strycharz et al., 2019a). Thus, to advance theory and provide more insight to communication professionals and the privacy debate, the current study aims to validate the Perceived Surveillance Scale.

Validation Strategy

The Perceived Surveillance Scale

In the current study, we validated the Perceived Surveillance Scale used in prior research (e.g., Segijn et al., 2021; Segijn & van Ooijen, 2020; Sifaoui et al., 2022). Participants are asked to rate to what extent they believe that companies are 1) *watching your every move*, 2) *checking up on you*, 3) *looking over your shoulder*, and 4) *entering your private space* (Table 1). These items of the Perceived Surveillance Scale were developed based on qualitative interviews published by Phelan et al. (2016). In this study, they conducted 23- to 56-minute semi-structured interviews with 37 undergraduate students to study the role of individuals' privacy concerns in their information disclosure decisions. A quote by a participant that illustrates perceived surveillance is "However, it's just, like, a weird thing to think about, that someone's sort of watching you, whatever you're doing" (Phelan et al., 2016, p. 5246). In addition, a participant mentioned, "I didn't want to have something checking up on me" (p. 5247). Each of these quotes are reflected in two items of the scale, two that used the language of the quotes directly (respectively "watching your every move" and "checking up on you") and two items that are in line with these first quotes (respectively "looking over your shoulder" and "entering your private space").

We tested the four items of the Perceived Surveillance Scale in three separate studies. The first data set contained pilot survey data of 137 U.S. students aged 18 and over (Study 1). This pilot study was the first in which the Perceived Surveillance Scale was used. The aim of this study was to determine the scale's factorial structure, validity, and reliability. The second data set contained survey data from 1,008 U.S. respondents aged 18 to 94 (Study 2). This study aimed to determine whether the factorial structure, validity, and reliability could be replicated in a general sample, making the scale suitable for surveys among diverse audiences (i.e., in terms of education and age). Finally, the third data set contained data from an online scenario-based experiment conducted among 527 U.S. respondents aged 18 to 86 (Study 3). This study allowed us to test whether the scale could be corroborated for experimental research as well.

Table 1. *The Perceived Surveillance Scale.*

Study 1 and 2		
To what extent do you believe this strategy to sync advertisements stimulates the feeling that companies are…		
	Watching your every move	1: *Not at all*, 7: *Very much*
	Checking up on you	1: *Not at all*, 7: *Very much*
	Looking over your shoulder	1: *Not at all*, 7: *Very much*
	Entering your private space	1: *Not at all*, 7: *Very much*
Study 3		
When I imagine the media situations presented earlier happening to me, I would feel that advertising companies were…		
	Watching your every move	1: *Strongly disagree*, 7: *Strongly agree*
	Checking up on you	1: *Strongly disagree*, 7: *Strongly agree*
	Looking over your shoulder	1: *Strongly disagree*, 7: *Strongly agree*
	Entering your private space	1: *Strongly disagree*, 7: *Strongly agree*

In Studies 1 and 2, perceived surveillance was measured for six different personalization techniques that are often employed to personalize messages (Segijn & van Ooijen, 2020), namely, segmentation (also known as online profiling), social media analytics, geofencing, I.P. matching, keywords, and watermarking. The personalization techniques were shown one by one in random order and included a short explanation (Figure 1). After a brief description of the different personalization techniques, the respondents were asked their perceptions of surveillance of each technique separately (Table 1). For each personalization technique, the four items were

presented in random order. We used the loop and merged function in Qualtrics to randomize the strategies and piped text to insert the data collection method and description (Figure 1). In Study 3, a similar measurement was used to measure perceived surveillance and then to measure perceived surveillance as a response to a personalized communication scenario instead of merely a description of personalization techniques. Participants in this study were exposed to either a personalized scenario based on their current media behavior (i.e., synced) or not (i.e., not synced). The Perceived Surveillance Scale was adapted to fit the context of this study (Table 1). We expect that participants who were exposed to a personalized message would experience higher levels of perceived surveillance.

Figure 1. *Loop and Merge and Piped Text in Qualtrics Study 1 and 2.*

	Field 1	Field 2
1	Social media analytics	Tracking hashtags on popular social media sites
2	Segmentation	Information about your demographics (e.g., age, gender), values, and lifestyle
3	Watermarking	Sound signal (watermark) from the media content that is picked up by your device
4	Geofencing	Tracking your location data and use this information to advertise based on your current location
5	IP-matching	Matching the IP addresses of the difference devices you own
6	Using key-words	Using pre-defined words to trigger a relevant ad on a mobile device

Construct Validation

A scale's construct validity can be demonstrated through its relationship to other concepts (Noar, 2003). Respondents' scale scores should relate to their scores on other scales measuring concepts known to be correlated. In all three studies, additional concepts were measured next to perceived surveillance to determine the scale's construct validity. In both Study 1 and Study 2, we examined the correlation between respondents' perceived surveillance scores on the one hand and general privacy concerns, perceived vulnerability, perceived severity, and attitudes toward personalization on the other hand. In Study 3, general privacy concerns were also measured. In addition, we included creepiness, trust, and privacy risk perception (as a second-order factor consisting of perceived susceptibility and perceived severity of privacy violations), and perceived personalization as validation measures (Table 2). Below, we discuss the anticipated positive relationships first and the anticipated negative effects second. In addition to the relationships with related concepts, we will also test the relationship with a similar construct (i.e., surveillance concerns, measured in Study 3).

Privacy Concerns, Perceived Vulnerability, Perceived Severity, Creepiness, and Perceived Personalization. First, we propose to test the positive relationship between perceived surveillance and privacy concerns, perceived vulnerability, perceived severity, creepiness, and perceived personalization (Table 2). We define privacy concerns as the degree to which an individual is worried about the potential invasion of the right to prevent personal information disclosure to others (Baek & Morimoto, 2012). As the literature indicates, the realization that one is being tracked often results in privacy concerns (Li, 2011) and privacy protective measures, such as blocking cookies, rejecting data collection request, or other measures that erase one's digital footprint (Acquisti et al., 2020; Dienlin & Trepte, 2015; Vitak, 2020; but also see Kokolakis, 2017, for a discussion on the relationship between privacy concerns and privacy behaviors). These findings suggest that the realization that one is being tracked or surveilled upon positively affects concerns about privacy. Moreover, as demonstrated by Nowak and Phelps (1992), individuals tend to be concerned about their online privacy especially when information is more directly traceable to the individual. As perceived surveillance implies the perception of one "looking over your shoulder", and therefore implies that an individual is observed more directly, we expect the concept to be positively related to privacy concerns.

Perceived vulnerability to a privacy threat is defined as the perceived likelihood that a privacy threat occurs (Maddux & Rogers, 1983), such as using one's data in ways that one could not foresee or inappropriate usage. Perceived vulnerability is a positive predictor of privacy protective behaviors (Aguirre et al., 2015; Ham, 2017; Mousavi et al., 2020). As perceived surveillance concerns the experience that another agent is watching over one's shoulder and therefore gaining access to one's personal information—for either known but sometimes also unknown purposes—we predict that perceived surveillance is positively related to perceived vulnerability. This

notion is also supported by earlier work by Dinev and Hart (2004), who found that perceived vulnerability is positively related to privacy concerns.

Based on Rogers' Protection Motivation Theory (Maddux & Rogers, 1983), the perceived severity of the privacy threat is defined as the perceived 'noxiousness' of a privacy threat in terms of one's (psychological) well-being (Aguirre et al., 2015). For instance, when individuals experience a high-severity privacy threat, they may feel exposed, unprotected, and intruded upon by others. Higher degrees of personalization in advertising have been shown to increase perceived severity among individuals (Aguirre et al., 2015). Similarly, we predict that the more an individual experiences surveillance, the higher perceived severity.

The creepiness of personalization practices is defined as "an emotional reaction to an experience, interaction, technology or unsolicited communication where personal information has been collected with or without your knowledge and used in an unexpected or surprising manner invoking negative feelings" (Stevens, 2016, p. 34). Furthermore, it is experienced by individuals in situations associated with invasion of privacy, stalking behavior, and violation of social norms (Moore et al., 2015). Considering the creepiness experience in situations associated with stalking behavior, we expect that perceived surveillance is positively related to creepiness.

Perceived personalization is the extent to which the receiver feels the message is tailored to a unique individual (Aguirre et al., 2015; Kalyanaraman & Sundar, 2006). When a receiver perceives a message as reflecting her interest more closely, this may elicit privacy concerns and reactance, especially when the sender is trusted less (Bleier & Eisenbeiss, 2015). Thus, it is about the receiver's perceptions rather than the actual personalization (Maslowska et al., 2011; Tran, 2017). Because perceived surveillance is proposed to be a result of personal data as input for personalized communication, it is proposed that perceived personalization and perceived surveillance are positively related.

Attitudes Towards Personalisation and Trust in Fair Use of Personal Data. Second, we argue that perceived surveillance has a negative relationship with attitudes toward personalization and trust in fair use of personal data. Attitudes toward personalization indicate the extent to which people feel positive or negative toward personalized advertising (Tran, 2017). It has been argued that personalized communication could have both benefits and costs for the media user (Awad & Krishnan, 2006; Dinev & Hart, 2006). Examples of benefits are that personalized communication would improve media experiences (McDonald & Cranor, 2010; Vesanen, 2007), saving time finding information or receiving more informative and relevant messages (Strycharz et al., 2019b). On the other hand, it could be considered as a cost because of concerns about one's privacy, or perceived risks of data disclosures (e.g., data breaches; Dinev & Hart, 2006). Perceived surveillance is seen as one of the costs of personalized communication (Segijn & van Ooijen, 2020). Thus, it is expected that when only perceived surveillance and attitudes towards personalization are taken into account, high levels of perceived surveillance are related to negative attitudes toward personalization and that low levels of perceived surveillance are related to more positive attitudes toward personalization. Therefore, we propose that perceived surveillance and attitudes toward personalization are negatively related.

In addition, trust in fair use of personal data reflects the degree to which people believe that an entity that collects and uses personal data will protect consumers' personal information (Bol et al., 2018; Metzger, 2004). The negative relationship between perceived surveillance and trust can be explained by social contract theory. According to this theory, entities that collect and use people's data are expected to treat these data responsibly through an implied social contract (Miyazaki, 2008; Moore et al., 2015). This social contract is based on a trust relationship on the fair use of data between the entities collecting and using the data and the people whose data are collected. Once people suddenly become aware of someone looking over their shoulder, surveillance could be perceived as a violation of that contract in which trust is broken. Therefore, we expect perceived surveillance to be negatively related to attitudes toward personalization and trust.

Surveillance Concerns. Finally, in Study 3, we also measured another scale used to measure perceived surveillance, which we will call 'surveillance concerns,' to prevent confusion between the validated scale and another measure of the same concept. The scale of surveillance concerns was developed—yet to our knowledge not validated—by Xu et al. (2012). The items consist of *I believe that the location of my mobile device is monitored at least part of the time*, *I am concerned that mobile apps are collecting too much information about me*, and *I am concerned that mobile apps may monitor activities on my mobile device*. Although the first item matches our conceptualization of perceived surveillance, the other two items seem to measure concerns related to data collection that might be more closely related to the concept of privacy concerns, which represents an individual's worries about organizational information privacy practices (Phelps et al., 2000; Smith et al., 1996), rather than an

individual's perceptions of being watched. However, given that it was conceptualized as a measure of perceived surveillance, we propose also to test the relationship between the developed Perceived Surveillance Scale and the surveillance concerns scale.

Data Analysis Strategy

For each study, the Perceived Surveillance Scale's factorial structure was assessed through a measurement model estimated using the maximum likelihood procedure in Amos 25. For a measurement model—or any structural equation model for that matter—to be interpreted, it is vital that it has a good fit to the data. In this manuscript, we examined our models' fit based on their CMIN/DF value, CFI value, and RMSEA value. CMIN/DF values should below 5.00, CFI values above .90, and RMSEA values below .08 indicate acceptable fit (Kline, 2015).

In the measurement models of Study 1 and Study 2 (Figure 2), perceived surveillance was modeled as a second-order concept with the perceived surveillance for each of the six different personalization strategies as underlying first-order concepts. The theoretical rationale for modeling the six personalization strategies as six separate first-order factors is that both communication professionals and researchers may use only one or a sub selection of techniques in their practices. The current models can reveal (a) how well the four items measure perceived surveillance for each respective personalization strategy and (b) how the level of perceived surveillance for each respective personalization strategy contributes to respondents' overall perceived surveillance. These are important insights because different personalization techniques may result in different levels of perceived surveillance (Segijn & van Ooijen, 2020). With this information in mind, communication professionals could reconsider which strategies they want to employ separately or combined, and researchers could decide to study differences in the effects of different personalization strategies.

Concretely, for Study 1 and 2, we modeled one latent variable per personalization technique, based on the four indicators of that particular personalization technique. The error terms of the same indicator (i.e., the first, second, third, and fourth) were allowed to correlate across all personalization techniques to account for shared measurement error (Kline, 2015). The measurement models for Studies 1 and 2 indicate whether (1) indicators have a significant factor loading on their designated factor and their designated factor only, meaning that (2) there are no cross-loading items contributing to two factors at the same time, making all the factors unique and making it possible to (3) examine construct validity for the six first-order concepts or the second-order factor separately. Or, put more simply, it means that (1) items only have a significant factor loading on the one personalization technique they are supposed to measure and (2) they have a non-significant factor loading on the five other personalization techniques, meaning that (3) all six personalization techniques are measured by an unique set of items, making it possible to study the six personalization techniques either separately or combined. In Study 3, perceived surveillance was modeled as a first-order factor because only one type of personalization strategy was included. All descriptive statistics, Cronbach's alpha coefficients, and the correlation coefficients needed to assess the reliability and construct validity of the Perceived Surveillance Scale(s) were obtained using IBM SPSS Statistics 25.

Table 2. *Overview of Constructs Related to Perceived Surveillance.*

Construct	Definition	Measure	Source/Adapted from	Expected relationship	Study
Privacy concerns	The degree to which a consumer is worried about the potential invasion of the right to prevent the disclosure of personal information to others.	• I feel uncomfortable when information is shared without my permission • I am concerned about misues of my personal information • It bothers me to receive too much advertising material of no interest • I believe that my personal information is often misused • I think campanies share my information without permission	Baek and Morimoto (2012)	Positive	1, 2, 3
Perceived vulnerability	The likelihood that a privacy threat occurs.	• My personal information could be misused • My personal information could be made available to unknown individuals or companies without my knowledge • My personal information could be made available to government agencies • My personal information could be inappropriately used • My personal data could be subjected to a malicious computer/information secirity problems (e.g., virus, privacy, identity theft, hacking etc.)[a] • My personal data could be used in ways I do not foresee[b]	Maddux and Rogers (1983)	Positive	1, 2
Perceived severity	The perceived "noxiousness" of a privacy threat in terms of one's (psychological) well-being.	When I realize that onine companies and advertising agencies have collected and use personal information about me, I feel… • exposed • unprotected • unsafe • susceptable • vulnerable	Aguirre et al. (2015)	Positive	1, 2
Privacy risk perception	Consist of the likelihood people attach to privacy breaches and the severity (perceived seriousness) of the privacy breaches.	I believe companies… • collect information about my TV viewing behavior • use my TV vwiting behavior to show me advertisements • share information about my TV viewing behavior with other companies I would find it problematic if companies would… • collect information about my TV viewing behavior • use my TV vwiting behavior to show me advertisements • share information about my TV viewing behavior with other companies	Bol et al. (2018)	Positive	3
Creepiness	An emotional reaction to an experience, interaction, technology, or unsolicited communication where personal information has been collected with or without your knowledge and used in an unexpected or surprising manner invoking negative feelings.	• It is unsettling to receive ads personalized based on my TV viewing habits • Ads personalized based on my TV viewing habits make me feel uneasy • I feel threatened by ads personalized based on my TV viewing habits • Ads personalized based on my TV viewing habits invade my privacy	Stevens (2016)	Positive	3

Perceived Personalization	Perceptions of the degree of personalization.	• The ads were based on the TV shows I watched as described in the previous media scenarios • The ads targetd me as a unique individual • The ads were based on my media use as described in the previous media scenario • The ads seemed to be desgined specifically for me	Kalyanarama and Sundar (2006)	Positive	3
Attitude towards personalization	How people feel towards personalized communication.	• I prefer that ads shown on my device are personalized to my interests • I find it useful that ads on my device offer discounts based on my interests • Nobody should use data aboyt my media use because they are private (R) • I dislike the idea of ads that are adjusted to my media use (R) • I prefer ads that are adjusted to my preferences • I dislike the diea that someone monitors my media use (R)	Tran (2017)	Negative	1, 2
Trust in fair use of personal data	The degree to which people believe that an entity will protect consumers' personal information.	• Advertising companies would be trustworthy in handling my information • Advertising companies would tell the truth and fulfill promises related to the information provided by me • I trust that advertising companies would keep my best interest in mind when dealing with the information • Advertising companies are in general predictable and consistent regarding the usage of information • Advertising companies are always honest with customers when it comes to using the information that I would provide	Bol et al. (2018); Malhotra et al. (2004)	Negative	3
Surveillance concerns	No definition provided by Xu et al. (2012). Surveillance is described as a dimension of concern for information privacy.	• I believe that my TV viewing habits are monitored at least part of the time • I am concerned that companies are collecting too much information about my TV viewing habits • I am concerned that companies may monitor my TV viewing habits	Xu et al. (2012)	Positive	3

Note. [a]Study 1 only, [b]Study 2 only, R = reversed item.

Study 1: Student Survey

The first study aimed to pilot test the survey and measures before testing it in the general sample survey (Study 2). The data of Study 1 have solely been used for this purpose and have not been published elsewhere.

Method

Participants

After obtaining IRB approval from a large midwestern university in the U.S., the survey was administered through the same university's subject pool in Spring 2019. Students could self-select by clicking on the link in the subject pool. After providing informed consent, they could proceed to the survey. In total, 137 students fully completed the survey for research credits. There were no missing values in this data set. The mean age of the sample was 20.540 (*SD* = 1.996; range 18–37), and 79.6% were female. The majority of students (81.8%) identified themselves as White/Caucasian. We also asked about the current class standing, and 10.9% were freshmen, 35.8% sophomore, 33.6% junior, 19% senior, and 0.7% other. In addition, 35.0% of the students indicated having some work experience (incl. internships) in advertising, marketing, or communication. In addition, 36.5% of the students indicated having someone close to them (e.g., a friend or family member) working in one of these industries.

Measures

The means, standard deviations, and Cronbach's alphas of perceived surveillance per personalization strategy and for all six personalization strategies combined are presented in Table 3. In addition, we asked about other privacy-related measures (Table 2).

General Privacy Concerns. First, we asked about the students' general privacy concerns with six items on a 7-point scale (1 = *strongly disagree*, 7 = *strongly agree*) by Baek and Morimoto (2012) (*M* = 5.313, *SD* = 0.958, α = .744). An example item is *I am concerned about misuse of my personal information*.

Perceived Vulnerability. Second, we asked about perceived vulnerability with five items on a 7-point scale (1 = *strongly disagree*, 7 = *strongly agree*) by Dinev and Hart (2005) (*M* = 5.823, *SD* = 1.055, α = .858). An example item is *I feel my personal information in my mobile device could be inappropriately used*.

Perceived Severity. Third, we asked about perceived severity using five items on a 7-point scale (1 = *not at all*, 7 = *very much*) by Aguirre et al. (2015). We asked, *When I notice that advertisements on my mobile device are personalized and based on my media usage, I feel…* 1) *exposed*, 2) *unprotected*, 3) *unsafe*, 4) *susceptible*, and 5) *vulnerable* (*M* = 4.492, *SD* = 1.409, α = .908).

Attitudes Toward Personalization. Finally, we measured attitudes toward personalization with six items on a 7-point scale (1 = *strongly disagree*, 7 = *strongly agree*; *M* = 4.178, *SD* = 0.985, α = .824). An example item is *I prefer that ads shown on my mobile device are personalized to my interests*. Three negatively phrased items were reverse coded.

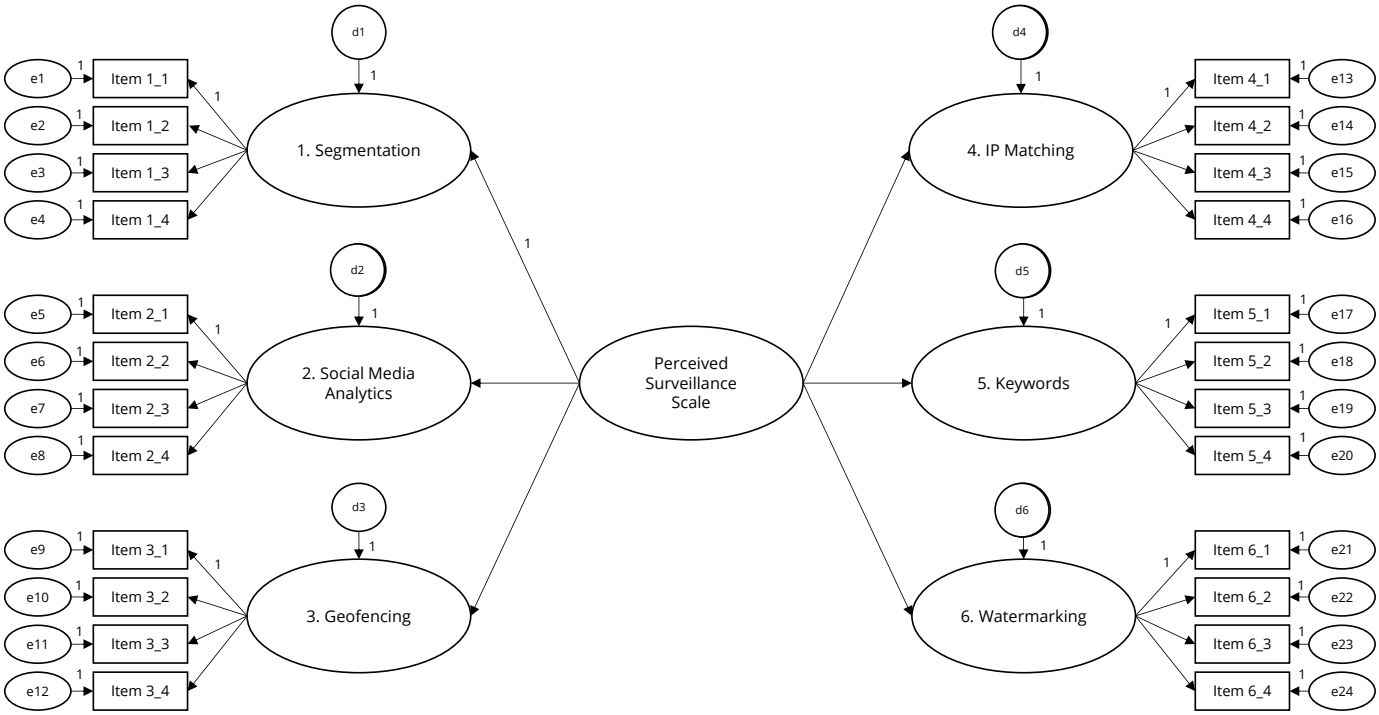
Table 3. *Descriptive Statistics of the Perceived Surveillance for Each of the Personalization Strategies.*

Personalization strategy	*M*	*SD*	Cronbach's α
1. Segmentation	3.489	1.698	.946
2. Social media analytics	3.287	1.733	.948
3. Geofencing	5.064	1.423	.920
4. IP matching	4.715	1.505	.934
5. Keywords	5.082	1.658	.934
6. Watermarking	5.909	1.407	.947
All (i.e., 1–6 combined)	4.591	1.009	.712

Results

The model (Figure 2) described in the data analysis strategy section had a good fit to the data: χ^2 (*df* = 198, *N* = 137) = 360.768 with $p < .001$, CMIN/DF = 1.822, CFI = .952, and RMSEA = .078, 90% CI [.065, .090]. Each indicator had a highly significant and strong factor loading on its designated factor (i.e., the standardized loadings varied from .812 to .945 with $p < .001$), and the model indices revealed that none of the indicators loaded onto a second factor (MIs ≤ 8.674 with SPECs ≤ .167; see Whittaker, 2012). This means that the Perceived Surveillance Scales for the six personalization strategies were unique and could be used independently. To verify whether their scores could also be combined into one higher-order factor, we examined the first-order latent scale variables' factor loadings onto the second-order latent scale variable. These were all highly significant, positive, and substantial, as the standardized loadings were successively .589, .461, .479, .710, .673, and .421 (with $p < .001$). Hence, it seems possible to use the second-order scale for subsequent analysis as well.

Figure 2*. Measurement Model for Study 1 and Study 2.*



Note. In the variable names following the format "Item X_X", the X before the underscore refers to the personalization technique, and the X after the underscore refers to the item number of the Perceived Surveillance Scale. Error terms associated with the same item number (e.g., denoted with e1, e5, e9, e13, e17, and e21 for item 1) were allowed to correlate.

As can be derived from Table 3, the Perceived Surveillance Scales for the six different personalization techniques had excellent reliability (i.e., α ≥ .920). The Perceived Surveillance Scale's reliability combining all techniques was somewhat lower but still satisfactory (i.e., α = .712). The various scales performed well in terms of construct validity. With the exception of only two non-significant correlations (i.e., between the perceived surveillance of social media analytics and perceived vulnerability and between the perceived surveillance of watermarking and attitudes toward personalization), all relationships were significant and in the expected direction (i.e., 26 in total, see Table 4). Because the size of the non-significant correlations exceeds .10, it is possible that they could become significant when the sample size is larger.

Table 4. *Bivariate Correlations (With p-Values) of the Perceived Surveillance for Each of the Personalization Strategies.*

Personalization strategy	General privacy concerns	Perceived vulnerability	Perceived severity	Attitude towards personalization
1. Segmentation	.337 (< .001)	.260 (.002)	.351 (< .001)	−.225 (.008)
2. Social media analytics	.273 (.001)	.150 (.080)	.242 (.004)	−.321 (< .001)
3. Geofencing	.307 (< .001)	.236 (.006)	.273 (.001)	−.198 (.020)
4. IP matching	.258 (.002)	.285 (.001)	.294 (< .001)	−.255 (.003)
5. Keywords	.190 (.026)	.289 (.001)	.234 (.006)	−.243 (.004)
6. Watermarking	.190 (.026)	.281 (.001)	.263 (.002)	−.121 (.159)
All (i.e., 1–6 combined)	.405 (< .001)	.386 (< .001)	.430 (< .001)	−.357 (< .001)

Study 2: General Sample Survey

As a second step, we validated the scale in a general survey sample. The survey used was largely the same as the survey in Study 1. Because the study was part of a broader project (see van Ooijen et al., 2022), the survey included several privacy measures. This study aimed to obtain insights into people's knowledge and perceptions of personalized advertising strategies, such as synced advertising (Segijn, 2019) and online behavioral advertising (Boerman et al., 2017; Varnali, 2019). IRB approval was obtained before conducting the study.

Method

Participants

The survey was administered through a renowned research panel Dynata (previously ResearchNow and Survey Sampling International (SSI)), between March and June 2019. Respondents received a survey invitation through the panel company to participate in the survey. After providing informed consent, they could proceed to the survey. In total, 1,008 U.S. respondents (55.8% female, age: *M* = 50.262, *SD* = 17.023; range 18–94 years) participated and passed at least three of the four attention checks. The attention checks included a combination of checking specific answer categories ('choose totally disagree'), an instructional manipulation check (Oppenheimer et al., 2009), and open-ended questions. The instructional manipulation check consisted of a filler scenario: "We are interested in whether you actually take the time to read the directions; if not, then some of our questions that rely on instructions will be ineffective. So, in order to demonstrate that you have read the instructions, please choose the (7) *Very likely to happen* option for scenario 3. Thank you very much." Participants who chose any other answer option were flagged but only removed if they did not pass other checks. In addition, participants who did not provide a cohesive answer (e.g., "dhfjkshd") to the open-ended questions were flagged as well but again only removed if they did not pass any of the other checks. At the end of the survey, the respondents were thanked for their participation and received a monetary incentive through the panel company for completing the survey.

Measures

The perceived surveillance measure was the same as in Study 1. The means, standard deviations, and Cronbach's alphas for each personalization strategy and all personalization strategies combined are presented in Table 5. Subsequently, we first asked about perceived vulnerability (*N* = 1,006, *M* = 6.083, *SD* = 1.150, α = .917), followed by perceived severity (*N* = 1,006, *M* = 5.727, *SD* = 1.340, α = .949). The question for perceived severity was now, *When I realize that online companies and advertising agencies have collected and used personal information about me, I feel…*. The answer options were the same as in Study 1. Privacy concerns were measured third (*N* = 1,007, *M* = 5.585, *SD* = 1.087, α = .870), and finally, we measured attitudes toward personalization similar to Study 1 (*N* = 1,005, *M* = 3.329, *SD* = 1.149, α = .797).

Table 5. *Descriptive Statistics of the Perceived Surveillance for Each of the Personalization Strategies Study 2.*

Personalization strategy	*N*	*M*	*SD*	Cronbach's α
1. Segmentation	1,006	5.031	1.692	.963
2. Social media analytics	1,007	5.179	1.704	.968
3. Geofencing	1,006	5.536	1.520	.957
4. IP matching	1,007	5.586	1.535	.959
5. Keywords	1,007	5.507	1.554	.958
6. Watermarking	1,007	5.829	1.448	.957
All (i.e., 1–6 combined)	1,003	5.443	1.259	.886

Results

The measurement model for Study 2 was fitted for all respondents with complete data on all the perceived surveillance items (Figure 2). The model had a good fit to the data: χ^2 (*df* = 198, *N* = 1,003) = 952.044 with $p < .001$, CMIN/*DF* = 4.808, CFI = .976, and RMSEA = .062, 90% CI [.058, .066]. Similar to Study 1, each indicator had a highly

significant and strong positive factor loading on its designated factor (i.e., the standardized loadings varied from .896 to .952 with $p < .001$), and the model indices revealed that none of the indicators loaded onto a second factor (MIs ≤ 20.536 with SPECs ≥ −.060). Furthermore, each first-order latent scale variable had a significant, positive, and substantial factor loading onto the second-order latent scale variable (successively .748, .726, .757, .775, .832, and .751 with $p < .001$). This meant that both the second-order and first-order scales could be used for further analysis.

As could be expected based on the higher factor loadings, the Perceived Surveillance Scales turned out to be even more reliable among the general sample: both the Perceived Surveillance Scales for the six different personalization techniques (i.e., α ≥ .957) and the overall Perceived Surveillance Scale had excellent reliability (i.e., α = .886). As previously, all scales performed well in terms of construct validity. This time, all 28 relationships were significant and in the expected direction (see Table 6).

Table 6. *Bivariate Correlations (all p < .001) of the Perceived Surveillance for Each of the Personalization.*

Personalization strategy	General privacy concerns	Perceived vulnerability	Perceived severity	Attitude towards personalization
1. Segmentation	.350	.261	.410	−.360
2. Social media analytics	.354	.256	.370	−.298
3. Geofencing	.425	.336	.454	−.378
4. IP matching	.425	.402	.493	−.362
5. Keywords	.371	.336	.354	−.334
6. Watermarking	.422	.392	.400	−.319
All (i.e., 1–6 combined)	.495	.418	.507	-.428

Note. The *n* differs due to missing data for some participants on some items between 1,001–1,007.

Study 3: Online Scenario-Based Experiment

Online scenario-based experiments are a common way to test personalization effects (for example, see Bleier & Eisenbeiss, 2015; Bol et al., 2018; Gironda & Korgaonkar, 2018). Therefore, it is important to validate the scale in this setting, as well. Moreover, validating the scale in an experimental setting will allow future research to test the effects of personalized messaging on perceived surveillance. We conducted secondary data analysis on data collected for a project that aimed to study synced advertising effects (Segijn & Kim, 2020) to validate the scale.

Method

Sample and Design

The study used the same data panel (i.e., Dynata) as in Study 2[1] and was conducted from October to November 2019. In total, 527 U.S. participants (48.8% female (0.4% other), age: $M = 46.411$, $SD = 17.037$; range 18–86 years) completed and passed at least three of the four attention checks. The attention checks included a combination of checking specific answer categories ('choose totally disagree'), self-reported attention to the study (50% or higher), and open-ended questions (similar to Study 2). At the end of the experiment, the participants were thanked for their participation and received an incentive through the panel company for completing the survey. Again, IRB approval was obtained before collecting the data.

After providing informed consent, participants could proceed to the experiment. They were asked to imagine themselves watching TV and using a smartphone at the same time. They received three different media scenarios, each describing a different TV show (i.e., a talk show, a game show, and a news program). Each TV show was accompanied by a picture of a smartphone screen that displayed an app (i.e., Sudoku app, weather app, and fit tracker app) and a banner ad at the bottom. The images of the smartphone were the same for all participants. The only difference was something mentioned in the TV scenario, which made the scenario and the product advertised in the banner ad either synced or not. Because each participant was randomly exposed to three

scenarios, they could be exposed to 0, 1, 2, or 3 synced scenarios. All materials for this study were selected based on multiple pretests.

Measures

See Table 2 for an overview of all measures. The same measure for privacy concerns was used as in the previous studies (N = 525, M = 5.485, SD = 1.229, α = .926). Because we conducted a secondary data analysis of a project, Study 3 contained different concepts related to perceived surveillance.

Perceived Surveillance. To measure perceived surveillance, the same four answer options were used as in the previous studies (Table 1), and they were measured on a 7-point scale (1 = *strongly disagree*, 7 = *strongly agree;* N = 526, M = 4.312, SD = 1.621, α = .936).

Creepiness. In addition, we measured creepiness with four items on a 7-point scale (1 = *strongly disagree*, 7 = *strongly agree*) by Stevens (2016) (N = 527, M = 4.728, SD = 1.568, α = .941). An example item is *Ads personalized based on my TV viewing habits make me feel uneasy*.

Trust in Fair Use of Personal Data. Furthermore, we measured trust with five items on a 7-point scale (1 = *strongly disagree*, 7 = *strongly agree*) by Malhotra et al. (2004) (N = 527, M = 3.479, SD = 1.537, α = .935). An example item is *Advertising companies would be trustworthy in handling my information*.

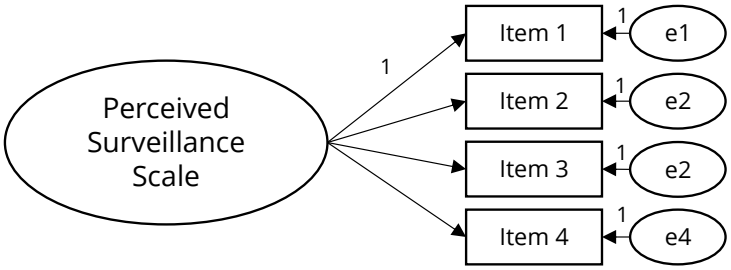
Surveillance Concerns. Next, we measured surveillance concerns with three items on a 7-point scale (1 = *strongly disagree*, 7 = *strongly agree*) by Xu et al. (2012; N = 526, M = 4.859, SD = 1.454, α = .894). An example item is *I believe that my TV viewing habits are monitored at least part of the time*.

Privacy Risk Perception. We measured privacy risk perception, and similar to Bol et al. (2018), it was measured as a second-order factor consisting of perceived susceptibility to privacy violations (N = 527, M = 5.057, SD = 1.341, α = .923) and perceived severity (i.e., seriousness) of privacy violations (N = 527, M = 5.254, SD = 1.420, α = .937; r = .539 with p < .001, N = 527, M = 5.156, SD = 1.211).

Results

The measurement model for Study 3 was fitted for all respondents with complete data on all the perceived surveillance items (Figure 3). The model had a good fit to the data: χ^2 (df = 2, N = 526) = 3.199 with p = .202, CMIN/DF = 1.599, CFI = .999, and RMSEA = .034, 90% CI [.000, .099]. All four indicators of perceived surveillance had highly significant, positive, and strong factor loadings (i.e., .933, .785, .955, and .874, respectively, all p < .001). Hence, in its new application, the scale maintained its factorial structure. All four items were important in measuring the concept. As presented above, the Perceived Surveillance Scale had excellent reliability (i.e., α = .936). Furthermore, after inspecting the bivariate correlations, we may once more conclude that it performs well in terms of construct validity. As expected, significant positive correlations were found between perceived surveillance and creepiness (n = 526, r = .509 with p < .001), surveillance concerns (n = 525, r = .426 with p < .001), privacy risk perception (n = 526, r = .429 with p < .001), and privacy concern (n = 524, r = .277 with p < .001). Finally, we found a significant but opposite effect for trust (n = 526, r = .095 with p = .029).

Figure 3. *Measurement Model for Study 3.*



Note. The items refer to participants' responses to the question *When I imagine the media situations presented earlier happening to me, I would feel the advertising companies were… watching your every move, checking up on you, looking over your shoulder,* and *entering your private space*.

Discussion

Due to the increasing sophistication of data-driven technologies, techniques, and algorithms that use people's online and offline personal data for input to create and distribute communication messages (Yun et al., 2020), companies have an improved ability to monitor and track media users. The rise of new information and communication technologies have contributed to making surveillance through collecting people's information easier and more accessible (Manokha, 2018). Related to this, the concept of perceived surveillance has become increasingly important when studying data-driven communication. In particular, the feeling of being watched affects people's media use, such as using less media, using media differently, or consuming different media content (Büchi et al., 2020; McDonald & Cranor, 2010; Stiff, 2019; Strycharz et al., 2022). Despite the growing importance of this concept to advance theory on data-driven practices, the practical implications related to personalized communication and privacy, and use of the scale in prior research, to our knowledge, no validated scale of perceived surveillance exists. However, to obtain more insights into the role of perceived surveillance in perceptions and acceptance of data-driven communication, it is important to have such a validated scale. Therefore, the current study aimed to validate the Perceived Surveillance Scale that could be used to study perceptions (survey research) and the effects of (experimental research) data-driven communication.

To validate the Perceived Surveillance Scale, we examined the items used in previous research based on qualitative interviews by Phelan et al. (2016). We tested the scale's reliability and construct validity in three different data sets. The first two data sets were surveys of which one was conducted among students and the other among a general U.S. population. The third data set was from a scenario-based experiment conducted among a general U.S. population. In all three studies, the Perceived Surveillance Scale showed good to excellent reliability and construct validity. The scale appeared to be reliable and valid in measuring perceived surveillance as perceptions of personalized communication and personalization techniques (i.e., segmentation, social media use, geofencing, I.P. matching, keywords, watermarking; see Studies 1 and 2), as well as perceived surveillance as an effect of personalized communication (see Study 3). Admittedly, the question and answer format of the Perceived Surveillance Scale differed between Study 1 and 2 on the one hand and Study 3 on the other hand (i.e., unipolar vs. bipolar; Table 1). This means that the unipolar Perceived Surveillance Scale was found reliable and valid in two studies, and the bipolar Perceived Surveillance Scale in one.

In all three studies, construct validity was measured by examining the Perceived Surveillance Scale's relationship and supposedly related and frequently used concepts in personalized communication literature. As expected, the results showed that the Perceived Surveillance Scale was positively related to privacy concerns, privacy risk perception, perceived vulnerability, perceived severity, creepiness, surveillance concerns, and perceived personalization. In addition, the results showed that, in line with our expectations, the Perceived Surveillance Scale was negatively related to attitudes toward personalization. Contrary to the expectations, we found that trust in fair use of personal data was positively related to perceived surveillance. This can be explained by the concept of privacy cynicism (i,e., "an attitude of uncertainty, powerlessness, and mistrust toward the handling of personal data by digital platforms, rendering privacy protection subjectively futile", Hoffmann et al., 2016). When facing a privacy threat (Lutz et al., 2020; van Ooijen et al., 2022) such as perceived surveillance, people may use privacy cynicism as a coping mechanism. Hence, perceived surveillance may lead to increased privacy cynicism and a subsequent dismissal of the problem at hand—meaning that trust is not impaired.

Additionally, in Study 1, we found two non-significant relationships, namely, between the Perceived Surveillance Scale of social media use and perceived vulnerability and the first-order Perceived Surveillance Scale of watermarking and attitudes toward personalization. It might be possible that these relationships work differently for students compared to a general sample. However, given that the size of the non-significant correlations exceeds .10 and given the smaller sample size of the pilot study reported in Study 1 compared to Study 2 and 3 (respectively N = 137 vs. N = 1,008 vs. N = 527) in which the significant relationships were shown, it is very likely these non-significant relationships could be explained by the smaller sample size of this data set. Therefore, it is important that future studies utilizing this scale ensure enough power to test the proposed assumptions.

Future Applications of the Perceived Surveillance Scale

Based on the correlations of perceived surveillance in Study 1 and Study 2, we may conclude that our scale is valid for measuring perceived surveillance as perceptions of personalized communication and personalization techniques (i.e., segmentation, social media use, geofencing, I.P. matching, keywords, watermarking)—both

separately and combined. The significant correlations for the first-order factors show that the scale can measure people's perceived surveillance for a particular personalization technique, for instance, if one wishes to study the causes and consequences of perceived surveillance for the segmentation technique. The significant correlations for the second-order factor indicate that the scale can also be used to measure consumers' perceived surveillance across personalization techniques to obtain a more thorough understanding of their overall perceived surveillance within the general commercial media environment—which may, ultimately, be a better predictor for their media use. In addition to the survey uses discussed above, the correlations in Study 3 showed that our scale of perceived surveillance is also valid for studying perceived surveillance as an effect of personalized communication within experimental settings.

The Perceived Surveillance Scale can be used to explain differences in perceptions of or responses to data-driven communication, such as personalized communication, computational advertising, or algorithmic decision making. The scale can be used to study the perceptions of and respond to data-driven practices in different research domains, such as political microtargeting, personalized advertising, and tailored health messages. Moreover, the scale could also be used to measure how individuals respond to new 'assistance' technologies that track them (Frick et al., 2021), such as smartwatches, home assistants, conversational voice agents, smart thermostats, and smart doorbells. Future research is needed to validate the scale in these contexts, as well as testing it in contexts that go beyond data-driven communication by corporations, for example, as a result of government surveillance (Penney, 2017) or in mediated communication (Ruggieri et al., 2021), such as perceived surveillance on social networking sites (Marwick, 2012). Additionally, surveillance is not just about knowing things about people, but it is used with the aim to control and influence those that are under surveillance (Lyon, 2002; Solove, 2006). For example, surveillance can be used for optimizing communication with the aim to persuade or sell but also for risk analytics, fraud detection, and pricing to name a few (Christl, 2017). The Perceived Surveillance Scale merely focuses on the perception of surveillance. Whether the aim of surveillance is known to people and how a specific aim affects subsequent perceptions or responses is something that future research should look into.

The Perceived Surveillance Scale can also be used to study *responses to* data-driven communication. This creates the possibility of using the measure in experimental research to study the effects of data-driven communication (e.g., personalized communication, computational advertising, algorithmic decision making) on perceived surveillance as well as using perceived surveillance as an underlying mechanism of data-driven communication on other outcomes. For example, perceived surveillance has been proposed as an underlying mechanism of resistance toward personalized communication (Farman et al., 2020) or to mediate the effects on affective (e.g., attitudes) and behavioral (e.g., click-through rates) responses to personalized communication (Segijn, 2019). An extensively studied behavioral response in the context of personalized communication is information disclosure (e.g., Bol et al., 2018; Masur & Scharkow, 2016; Mesch & Beker, 2010; Metzger, 2004). The validated scale allows researchers to provide new insights into information disclosure by studying perceived surveillance as an underlying mechanism of the effects.

The validation of the Perceived Surveillance Scale also has important implications for advancing knowledge for communication professionals. First, it could provide them with more information on the effectiveness of political microtargeting, personalized advertising, or a tailored health communication campaign. Personalization is argued to be effective when perceived benefits outweigh the perceived costs (Dinev & Hart, 2006). Thus, measuring perceived surveillance as an additional cost of personalization allows us to provide further insight into its potential effectiveness. Moreover, perceived surveillance negatively affects personalization outcomes (e.g., attitudes and behavioral intentions) because perceived surveillance increases resistance to a personalized message (Farman et al., 2020). Thus, although personalization is thought to be a more effective way to communicate than non-personalized messages because it allows for more precise targeting (Kumar & Gupta, 2016), it also has its own limitations. The Perceived Surveillance Scale's development allows practitioners to gain more insight into the effectiveness and potential barriers to personalized communication and other forms of data-driven communication.

Second, the Perceived Surveillance Scale's development allows communication professionals to gain more insight into how surveillance could affect people's media use. For example, internet users report changing their online behavior (e.g., not visiting certain websites) when they know their data are being collected; McDonald & Cranor, 2010). This phenomenon of refraining from consuming certain media (e.g., not browsing internet pages, not watching TV shows) due to perceived surveillance is known as a 'chilling effect' and has been identified as an ethical side effect of surveillance (Büchi et al., 2020, 2022; Finn & Wadhwa, 2014; Manokha, 2018; Solove, 2006). Moreover, because personalized communication's effectiveness depends on the quality of the data collected (e.g., people's

actual preferences; Strycharz et al., 2019a), self-surveillance practices could lower the quality of communication messages. Therefore, gaining more insights into how perceived surveillance affects people's media use (e.g., consuming less media, different media) is crucial to practitioners who design an effective personalized communication campaign.

Although the development of this scale has important implications for advancing people's knowledge of perceptions and responses to personalized communication, it should be acknowledged that all data that were used to validate the Perceived Surveillance Scale originated from studies conducted in the U.S. Data from other countries are necessary to obtain a better understanding of perceptions and effects of personalized communication. Especially given that privacy regulations differ between countries, which impacts how personal data are collected and treated (Strycharz et al., 2020), it is important to examine the concept outside the U.S. as well. For example, a key goal of the European General Data Protection Regulation is to strengthen individuals' control over their personal data (Strycharz et al., 2020; van Ooijen & Vrabec, 2019), which stands in contrast to the privacy regulations in the United States (with the exception of the California Consumer Privacy Act). When people experience more control over their data, surveillance perceptions might be different, or perceived surveillance might have different consequences for accepting surveillance. Therefore, we propose that future research will work toward validating the scale in a more international context. This will allow future research to compare perceived surveillance in the context of data-driven communication across countries and provide insights into whether the results of current cross-country studies can be directly compared.

Conclusion

The Perceived Surveillance Scale's development creates important new and timely avenues for studying data-driven communication. It will contribute to the advancement of theory by providing opportunities to study antecedents of perceptions and acceptance of data-driven communication and provide important implications for practitioners, as well as governmental regulations related to possible (un)wanted consequences of data collection practices for individuals.

Footnotes

[1] Given that the data of Study 3 was used for secondary data analysis we did not exclude any participants that participated in Study 2. Overlap in the samples is possible but we cannot check for that. However, both studies have a relatively small size compared to the total number of panelists in Dynata. Moreover, both studies include different constructs that were measured for construct validity, as well as the aim of both studies as presented to the participants were different. Therefore, we do not see this as a limitation of the study.

Conflict of Interest

The authors have no conflicts of interest to declare.

Authors' Contribution

Claire M. Segijn: conceptualization, methodology, resources (data), writing - original draft. **Suzanna J. Opree**: formal analysis, methodology, writing – original draft. **Iris van Ooijen**: conceptualization, resources (data), writing – review & editing.

Acknowledgements

The authors would like to thank Eunah Kim for her help with the original data collection of Study 3.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *ICIS 2006 Proceedings* (Article 94). AIS eLibrary. https://aisel.aisnet.org/icis2006/94

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology, 30*(4), 736–758. https://doi.org/10.1002/jcpy.1191

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34–49. https://doi.org/10.1016/J.JRETAI.2014.09.005

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13–28. https://doi.org/10.2307/25148715

Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of Advertising*, *41*(1), 59–76. https://doi.org/10.2753/JOA0091-3367410105

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing, 91*(3), 390–409. https://doi.org/10.1016/j.jretai.2015.04.001

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, *46*(3), 363–376. https://doi.org/10.1080/00913367.2017.1339368

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Bol, N., Smit, E. S., & Lustria, M. L. A. (2020). Tailored health communication: Opportunities and challenges in the digital era. *Digital Health, 6,* Article 2055207620958913*.* https://doi.org/10.1177/2055207620958913

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society*, *9*(1), 1–14. https://doi.org/10.1177/20539517211065368

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review, 36*, Article 105367. https://doi.org/10.1016/j.clsr.2019.105367

Byers, D. (2018, March 19). *Facebook is facing an existential crisis.* CNN. https://money.cnn.com/2018/03/19/technology/business/facebook-data-privacy-crisis/index.html

Christl, W. (2017). *Corporate surveillance in everyday life. How companies collect, combine, analyze, trade, and use personal data on billions*. Cracked Labs. https://crackedlabs.org/en/corporate-surveillance

De Keyzer, F., Dens, N., & De Pelsmacker, P. (2015). Is this for me? How consumers respond to personalized advertising on social network sites. *Journal of Interactive Advertising*, *15*(2), 124–134. https://doi.org/10.1080/15252019.2015.1082450

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. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7–29. https://doi.org/10.2753/JEC1086-4415100201

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

Duffy, B. E., & Chan, N. K. (2019). "You never really know who's looking": Imagined surveillance across social media platforms. *New Media & Society*, *21*(1), 119–138. https://doi.org/10.1177/1461444818791318

Farman, L., Comello, M. L., & Edwards, J. R. (2020). Are consumers put off by retargeted ads on social media? Evidence for perceptions of marketing surveillance and decreased ad effectiveness. *Journal of Broadcasting & Electronic Media*, *64*(2), 298–319. https://doi.org/10.1080/08838151.2020.1767292

Feezell, J. T., Wagner, J. K., & Conroy, M. (2021). Exploring the effects of algorithm-driven news sources on political behavior and polarization. *Computers in Human Behavior, 116*, Article 106626. https://doi.org/10.1016/j.chb.2020.106626

Finn, R. L., & Wadhwa, K. (2014). The ethics of "smart" advertising and regulatory initiatives in the consumer intelligence industry. *Info*, *16*(3), 22–39. https://doi.org/10.1108/info-12-2013-0059

Frick, N. R. J., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications, 47*, Article 101046. https://doi.org/10.1016/j.elerap.2021.101046

Gironda, J. T., & Korgaonkar, P. K. (2018). iSpy? Tailored versus invasive ads and consumers' perceptions of personalized advertising. *Electronic Commerce Research and Applications*, *29*, 64–77. https://doi.org/10.1016/j.elerap.2018.03.007

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

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), Article 7. https://doi.org/10.5817/cp2016-4-7

Hudders, L., van Reijmersdal, E. A., & Poels, K. (2019). Editorial: Digital advertising and consumer empowerment. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 13*(2), Article 1. https://doi.org/10.5817/CP2019-2-xx

Huh, J., & Malthouse, E. C. (2020). Advancing computational advertising: Conceptualization of the field and future directions. *Journal of Advertising, 29*(4), 367–376. https://doi.org/10.1080/00913367.2020.1795759

Kalyanaraman, S., & Sundar, S. S. (2006). The psychological appeal of personalized content in web portals: Does customization affect attitudes and behavior? *Journal of Communication*, *56*(1), 110–132. https://doi.org/10.1111/j.1460-2466.2006.00006.x

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. https://doi.org/10.5817/CP2016-1-2

Kim, H., & Huh, J. (2017). Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising*, *38*(1), 92–105. https://doi.org/10.1080/10641734.2016.1233157

Kline, R. B. (2015). *Principles and practices of structural equation modeling* (4th ed.). Guilford Publications.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kruikemeier, S., Sezgin, M., & Boerman, S. C. (2016). Political microtargeting: Relationship between personalized advertising on Facebook and voters' responses. *CyberPsychology, Behavior & Social Networking*, *19*(6), 367–372. https://doi.org/10.1089/cyber.2015.0652

Kumar, V., & Gupta, S. (2016). Conceptualizing the evolution and future of advertising. *Journal of Advertising*, *45*(3), 302–317. https://doi.org/10.1080/00913367.2016.1199335

Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011). Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection. *MIS Quarterly*, *35*(2), 423–444. https://doi.org/10.2307/23044050

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*(1), 453–496. https://doi.org/10.17705/1CAIS.02828

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

Lyon, D. (2002). Surveillance studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society*, *1*(1), 1–7. https://doi.org/10.24908/ss.v1i1.3390

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Manokha, I. (2018). Surveillance, panopticism and self-discipline. *Surveillance & Society, 16*(2), 219–237. https://doi.org/10.24908/ss.v16i2.8346

Marwick, A. E. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society, 9*(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Maslowska, E., Smit, E. G., & van den Putte, B. (2016). It is all in the name: A study of consumers' responses to personalized communication. *Journal of Interactive Advertising*, *16*(1), 74–85. https://doi.org/10.1080/15252019.2016.1161568

Maslowska, E., van den Putte, B., & Smit, E. G. (2011). The effectiveness of personalized e-mail newsletters and the role of personal characteristics. *Cyberpsychology, Behavior, and Social Networking*, *14*(12), 765–770. https://doi.org/10.1089/cyber.2011.0050

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, *2*(1), Article 205630511663436. https://doi.org/10.1177/2056305116634368

McDonald, A. M., & Cranor, L. F. (2010). Americans' attitudes about internet behavioral advertising practices. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society* (pp. 63–72). ACM. https://doi.org/10.1145/1866919.1866929

Mesch, G. S., & Beker, G. (2010). Are norms of disclosure of online and offline personal information associated with the disclosure of personal information online? *Human Communication Research*, *36*(4), 570–592. https://doi.org/10.1111/j.1468-2958.2010.01389.x

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4), Article JCMC942. https://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing*, *27*(1), 19–33. https://doi.org/10.1509/jppm.27.1.19

Moore, R. S., Moore, M. L., Shanahan, K. J., & Mack, B. (2015). Creepy marketing: Three dimensions of perceived excessive online privacy violation. *Marketing Management*, *25*(1), 42–53. http://www.mmaglobal.org/publications/mmj/current-past-issues/#collapseVol25-1

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, *135*, 113323. https://doi.org/10.1016/j.dss.2020.113323

Noar, S. M. (2003). The role of structural equation modeling in scale development. *Structural Equation Modeling*, *10*(4), 622–647. https://doi.org/10.1207/S15328007SEM1004_8

Nowak, G. J., & Phelps, J. E. (1992). Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing, 6*(4), 28–39. https://doi.org/10.1002/dir.4000060407

Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, *45*(4), 867–872. https://doi.org/10.1016/j.jesp.2009.03.009

Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review, 6*(2), 1–39. https://doi.org/10.14763/2017.2.692

Phelan, C., Lampe, C., & Resnick, P. (2016). It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 5240–5251). ACM. https://doi.org/10.1145/2858036.2858381

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Ruggieri, S., Bonfanti, R. C., Passanisi, A., Pace, U., & Schimmenti, A. (2021). Electronic surveillance in the couple: The role of self-efficacy and commitment. *Computers in Human Behavior, 114,* Article 106577. https://doi.org/10.1016/j.chb.2020.106577

Segijn, C. M. (2019). A new mobile data driven message strategy called synced advertising: Conceptualization, implications, and future directions. *Annals of the International Communication Association*, *43*(1), 58–77. https://doi.org/10.1080/23808985.2019.1576020

Segijn, C. M. & Kim, E. (2020, August 6–9). *Am I being watched? The role of perceived surveillance and privacy cynicism in synced advertising effects* [Conference presentation]. The annual conference of the Association for Education in Journalism and Mass Communications, virtual conference. https://convention2.allacademic.com/one/aejmc/aejmc20/

Segijn, C. M., Kim, E., Sifaoui, A., & Boerman, S. C. (2021). When realizing that Big Brother is watching you: The empowerment of the consumer through synced advertising literacy. *Journal of Marketing Communications*. Advance online publication. https://doi.org/10.1080/13527266.2021.2020149

Segijn, C. M., & van Ooijen, I. (2020). Perceptions of techniques used to personalize messages across media in real time. *Cyberpsychology, Behavior, and Social Networking, 23*(5), 329–337. https://doi.org/10.1089/cyber.2019.0682

Sifaoui, A., Lee, G., & Segijn, C. M. (2022). Brand match vs. mismatch and its impacts on avoidance through perceived surveillance in the context of synced advertising. In A. Vignolles (Ed.), *Advances in Advertising Research* (Vol. XII). Springer-Gabler.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560. https://doi.org/10.2307/40041279

Stevens, A. M. (2016). *Antecedents and outcomes of perceived creepiness in online personalized communications* [Unpublished doctoral dissertation]. Case Western Reserve University.

Stiff, C. (2019). The dark triad and Facebook surveillance: How machiavellianism, psychopathy, but not narcissism predict using Facebook to spy on others. *Computers in Human Behavior, 94*, 62–69. https://doi.org/10.1016/j.chb.2018.12.044

Strycharz, J., Ausloos J., & Helberger, N. (2020). Data protection or data frustration? Individual perceptions and attitudes towards the GDPR. *European Data Protection Law Review. 6*(3), 407–421. https://doi.org/10.21552/edpl/2020/3/10

Strycharz, J., Kim, E., & Segijn, C. M. (2022). Why people would (not) change their media use in response to perceived corporate surveillance. *Telematics & Informatics*, *71*, 101838. https://doi.org/10.1016/j.tele.2022.101838

Strycharz, J., van Noort, G., Helberger, N., & Smit, E. G. (2019a). Contrasting perspectives – practitioner's viewpoint on personalised marketing communication. *European Journal of Marketing, 53*(4), 635–660. https://doi.org/10.1108/EJM-11-2017-0896

Strycharz, J., van Noort, G., Smit, E. G., & Helberger, N. (2019b). Consumer view on personalized advertising: Overview of self-reported benefits and concerns. In E. Bigne, & S. Rosengren (Eds.), *Advances in Advertising Research X* (pp. 53–66). SpringerLink.

Tran, T. P. (2017). Personalized ads on Facebook: An effective marketing tool for online marketers. *Journal of Retailing and Consumer Services*, *39*, 230–242. https://doi.org/10.1016/j.jretconser.2017.06.010

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

van Ooijen, I., Segijn, C. M., & Opree, S. J. (2022). Privacy cynicism and its role in privacy decision-making. *Communication Research*. Advance online publication. https://doi.org/10.1177/00936502211060984

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, *42*(1), 91–107. https://doi.org/10.1007/s10603-018-9399-7

Varnali, K. (2019). Online behavioral advertising: An integrative review. *Journal of Marketing Communications, 27*(1), 93–114. https://doi.org/10.1080/13527266.2019.1630664

Vesanen, J. (2007). What is personalization? A conceptual framework. *European Journal of Marketing*, *41*(5/6), 409–418. https://doi.org/10.1108/03090560710737534

Vitak, J. (2020). Feature creep or just plain creepy? How advances in "smart" technologies affect attitudes toward data privacy. *Annals of the International Communication Association.* Advance online publication. https://par.nsf.gov/servlets/purl/10176663

Whittaker, T. A. (2012). Using the modification index and standardized expected parameter change for model modification. *The Journal of Experimental Education*, *80*(1), 26–44. https://doi.org/10.1080/00220973.2010.531299

Winter, S., Maslowska, E., & Vos, A. L. (2021). The effects of trait-based personalization in social media advertising. *Computers in Human Behavior*, *114*, Article 106525. https://doi.org/10.1016/j.chb.2020.106525

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In *Proceedings of the 33rd International Conference on Information Systems (ICIS): IS Security and Privacy* (Article 10). AIS eLibrary. https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10

Yun, J. T., Segijn, C. M., Pearson, S., Malthouse, E. C., Konstan, J. A., & Shankar, V. (2020). Challenges and future directions of computational advertising measurement systems. *Journal of Advertising*, *49*(4), 446–458. https://doi.org/10.1080/00913367.2020.1795757

Zarouali, B., Boerman, S. C., & de Vreese, C. H. (2021). Is this recommended by an algorithm? The development and validation of the Algorithmic Media Content Awareness Scale (AMCA-scale). *Telematics and Informatics, 62,* Article 101607. https://doi.org/10.1016/j.tele.2021.101607

Zarouali, B., Dobber, T., De Pauw, G., & de Vreese, C. (2020). Using a personality-profiling algorithm to investigate political microtargeting: Assessing the persuasion effects of personality-tailored ads on social media. *Communication Research*. Advance online publication. https://doi.org/10.1177/0093650220961965

Zhu, Y.-Q., & Chang, J.-H. (2016). The key role of relevance in personalized advertisement: Examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions. *Computers in Human Behavior*, *65*, 442–447. https://doi.org/10.1016/j.chb.2016.08.048

About Authors

Claire M. Segijn (PhD, University of Amsterdam) is an Associate Professor of Advertising and Mithun Program Fellow at the Hubbard School of Journalism and Mass Communication, University of Minnesota. Her research focuses on information processing and effectiveness of using multiple media at the same time (e.g., multiscreening, synced advertising). In line with that, she studies the intended and unintended effects (e.g., ethical ramifications of corporate surveillance) of personalized communication.

Suzanna J. Opree (PhD, University of Amsterdam) is an Associate Professor of Quantitative Methods in the Department of Media and Communication at the Erasmus School of History, Culture and Communication in Rotterdam. Her research line, "The good(s) life," focuses on the effects of advertising and commercial media on youth's materialism and well-being.

Iris van Ooijen (PhD, University of Amsterdam) is an Assistant Professor of Communication Science at the Behavioral Science Institute, Radboud University, Nijmegen. Her research includes (consumer) behavior in the context of new technologies, with a focus on privacy behaviors and responses to data-collecting technologies.

✉ **Correspondence to**
Claire M. Segijn, Ph.D., Hubbard School of Journalism and Mass Communication, University of Minnesota, 206 Church St. SE, 111 Murphy Hall, Minneapolis, MN, 55455, United States, segijn@umn.edu