



UvA-DARE (Digital Academic Repository)

Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns

Dobber, T.; Trilling, D.; Helberger, N.; de Vreese, C.

DOI

[10.1177/1461444818813372](https://doi.org/10.1177/1461444818813372)

Publication date

2019

Document Version

Final published version

Published in

New Media & Society

License

CC BY-NC

[Link to publication](#)

Citation for published version (APA):

Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. (2019). Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns. *New Media & Society*, 21(6), 1212-1231. <https://doi.org/10.1177/1461444818813372>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (<https://dare.uva.nl>)



Article

Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns

new media & society
2019, Vol. 21(6) 1212–1231
© The Author(s) 2018



Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1461444818813372
journals.sagepub.com/home/nms



Tom Dobber , Damian Trilling,
Natali Helberger and Claes de Vreese

University of Amsterdam, The Netherlands

Abstract

Tailored political messages are increasingly prevalent in election time, but we know little about how people perceive such data-driven and potentially privacy-infringing techniques. This article examines how demographics relate to privacy concerns and attitudes toward “political behavioral targeting” (PBT), how privacy concerns and attitudes toward PBT relate over time, and explore their relation with autonomy, electoral deliberation, and chilling effects. Using a three-wave panel study, administered in the Netherlands ($N=879$), we examine a potential reciprocal relation between attitude toward PBT and privacy concerns, which may form a negative reinforcing spiral dynamic over time. This dynamic could result in undesirable behavior of the voter from a democratic viewpoint (e.g. chilling effects). We find that demographics fall short in explaining privacy concerns. More importantly, we find evidence for a reinforcing spiral dynamic and, by doing so, contribute to the discussion about the threats and promises of PBT to society.

Keywords

Attitudes, campaigns, microtargeting, political behavioral targeting, privacy concerns

Corresponding author:

Tom Dobber, Amsterdam School of Communication Research, University of Amsterdam, Nieuwe Achtergracht 166, 1018 WV Amsterdam, The Netherlands.
Email: t.dobber@uva.nl

Introduction

As people increasingly use online services, and leave digital traces, it becomes easier to build data-rich profiles of ordinary citizens. Such profiles allow political advertisers to segment the electorate and to target specific groups of voters with tailored messages. The use of this technique, “political behavioral targeting” (PBT), is widespread in the United States (e.g. Hersh, 2015; Kreiss, 2016; Nielsen, 2012) and emerging in European democracies (Anstead, 2017; Dobber et al., 2017).

Proponents emphasize that tailoring may lead to voters receiving messages about topics they actually care about. Critics worry about citizens’ privacy (Bennett, 2015; Howard, 2006; Tene, 2011) and the information asymmetry between political campaigns and citizens (Tufekci, 2014). Campaigns can base their actions on personal data, while the receiver is unaware on the basis of what data she is being targeted (*if she is at all aware that she is being targeted*). This could open the door to voter manipulation (Zuiderveen Borgesius et al., 2018).

Learning about PBT, or noticing, for example, that a campaign “knows” what websites you have visited recently, can induce privacy concerns. These concerns, in turn, can result in a negative attitude toward the use of PBT techniques by political campaigns. This process is likely reciprocal: A more unfavorable attitude toward PBT might also lead to more privacy concerns. Together, privacy concerns and attitude toward PBT may form a reinforcing spiral, each influencing the other over time. As a result, a voter may experience so-called chilling effects. A chilling effect occurs when voters refrain from certain behavior because they perceive they are being monitored (Marder et al., 2016; Penney, 2016). A voter may, for example, not seek out information about the standpoints of certain political parties on specific topics because she feels she is being watched, or because she fears third parties can use her information seeking behavior to infer private information. These topics need not be controversial (although they might be). Voters may refrain from seeking out information about (somewhat) controversial standpoints, simply because the *future* consequences of looking up such information remain unclear. Considering the accuracy of computer-based judgments, such fear is not unwarranted (Youyou et al., 2015). Furthermore, a relation between privacy concerns and chilling effects has been found in commercial online behavioral advertising: people self-reported that they would be “more careful online” or “self-censor if they knew advertisers were collecting data” (McDonald and Cranor, 2010: 22). Moreover, as attitudes are predictors of behavior (Millar and Tesser, 1989), it is important to examine people’s attitudes, and, in this case, also the reciprocal process between attitude and privacy concerns. An occurrence of chilling effects in commercial advertising is undesirable (for the consumer *and* the advertiser), but chilling effects taking place during a citizen’s process of free and private deliberation to reach an informed voting decision can be detrimental to the electoral process. Without the experience of a private space, after all, a citizen is hindered in her ability to “reflect on and entertain beliefs, and to experiment with them” (Reiman, 1995: 42), which hampers her ability to reach an informed voting decision. Of course, apart from chilling effects, there are other examples of potential detrimental consequences. Political campaigns using PBT techniques to reach and persuade voters who perceive PBT unfavorably may fuel voter distrust

(Turow et al., 2012) and threaten voters' intellectual privacy (see Richards, 2015). Moreover, demographics may play a role in predicting privacy concerns or attitudes toward PBT.

We look at the relationship between demographics, on one hand, and privacy concerns and attitudes toward PBT, on the other, and then examine the reciprocal relation between these. We shed light on the potential reinforcing negative spiral, which can induce chilling effects during the voter's process of private deliberation. This means that we examine whether there are actual grounds for the existence of the chilling effects as described above,¹ through a repeated measurement panel survey ($N=879$, $T=3$). We try to answer the following overarching research question:

How does the Dutch electorate perceive PBT, and how do privacy concerns and attitude towards PBT influence each other over time?

The consequences of a reinforcing spiral on voter behavior are beyond the scope of this article. However, we have seen evidence of chilling effects following online behavioral advertising (McDonald and Cranor, 2010) and following online surveillance (Penney, 2016). Considering the importance of free and private electoral deliberation, we should not underestimate the potential threat a reinforcing spiral poses to the electoral process.

Theoretical background and related research on PBT in the United States and Europe

This study is part of an emergent field that examines data use by political campaigns. Recent approaches mainly focused on understanding the phenomenon and the mechanisms behind it (Anstead, 2017; Kreiss, 2012, 2016; Nielsen, 2012). These studies coincided with more descriptive accounts of data-driven political campaigning (e.g. Bimber, 2014, but also see Nickerson and Rogers, 2014, for an overview of microtargeting) and accompanied critical takes of the phenomenon and its threats to democratic societies (e.g. Barocas, 2012; Tufekci, 2014). All these studies have an Anglo-Saxon focus, which raises the question of whether political parties can "campaign in Europe as they do in North America?" (Bennett, 2016: 261). Bennett (2016) notes the relatively more stringent data protection regulations in Europe and observes that North American countries set the trend in data-driven campaigning, which, perhaps, should not be seen separately from each other. It must be noted that evidence in support of positive effects of microtargeting on voter behavior is sparse. Hersh and Schaffner (2013) found that voter groups prefer broad political appeals over tailored ones, and that political campaigns risk getting penalized when they mistarget an individual. Broockman and Green (2012) found that political ads, targeted via Facebook, did not improve candidate's name recognition or evaluations. However, likely due to advances in microtargeting and data analysis techniques, it has become easier to identify partisans. As such, Panagopoulos (2016) has signaled a move in US presidential campaigns back from persuasion efforts, toward mobilizing the base. Hersh (2015) has shown that US campaigns benefit less

from the messy commercial data they acquire from data brokers and more from publicly available data, especially voter records and census data. This is in line with a study by Endres (2016), who found that campaigns that could rely on a detailed voter file were able to microtarget voters more accurately than campaigns that could not rely on those data. However, “strict” European Union (EU) regulations prohibit a European variant of the US voter file. Yet, Dobber et al. (2017) found that political campaigns in Europe can still rely on other accurate public data (such as census data), just like their American counterparts can.

Not only advanced campaigns can use PBT: At the very least, less-advanced campaigns can fall back on Facebook, which offers a relatively cheap personalized advertising infrastructure. Intermediaries like Facebook hold different, more detailed, data of citizens than political campaigns do. As such, in Europe, too, citizens should be aware of the new data-driven political persuasion techniques and the value of their personal data to political campaigns. The extent to which citizens actually worry about their privacy and their personal data remains unclear. Turow et al. (2012) were early to survey the American electorate and discovered broad resistance against data-driven political campaigning techniques within the US electorate. However, these (somewhat outdated) US-based findings do not necessarily apply to Europe.

Privacy concerns and electoral deliberation

Being concerned about one’s privacy has negative consequences for citizens’ autonomy, and, by extension, on electoral deliberation. In the political realm, we view political autonomy as “the form of self-governance that one exercises together with others in authorizing laws and various forms of collective action” (Anderson, 2013: 454). Political autonomy requires self-constitution, independence, and rationality (Anderson, 2013). Being concerned about one’s privacy is especially problematic for citizens’ autonomy, we argue. People’s ability to take autonomous decisions is in jeopardy when anonymous third parties hold vast amounts of personal data that allow them to arbitrarily interfere in people’s lives and use that knowledge to manipulate them (see, for example, Pettit, 2017; Tene and Polonetsky, 2013). This situation can contribute to a sense of privacy concern, which worsens citizens’ *feeling of autonomy*. If someone expects, fears or is concerned about being sanctioned for holding an unpopular opinion, having privacy still enables that person to independently (but autonomously) form an unpopular opinion. When third parties amass personal data, and use that data to infer peoples’ opinions and behaviors, deviating from the popular opinions and behaviors becomes riskier. This development can be likened to the spiral of silence theory (Noelle-Neumann, 1974, but also Scheufele and Moy, 2000), but differences in that the spiral of silence results in not speaking out deviating opinions, while privacy concerns hamper individuals’ ability to deliberate independently (to independently *form* deviating opinions). As autonomous individuals form the heart of liberal democracy, we agree with Gavison’s (1980) observation: “To the extent that privacy is important for autonomy, it is important for democracy as well.” A citizen needs a “room to think for oneself,” to be able to develop her own political judgment (Dawes, 2014) and privacy concerns threaten the experience of such political privacy (p. 455).

As the degree to which someone is concerned about her privacy differs per person, we first look at antecedents. The literature suggests *gender*, *age*, *education*, and *knowledge* are predictors. Men are usually less worried about their privacy than women are (Baruh et al., 2017). The role of age is ambiguous. American-based research suggests all age groups have similar privacy concerns (Hoofnagle et al., 2010) and similar emotional responses to surveillance scenarios (Turow et al., 2018), while European-based research finds that older people are generally more concerned about their privacy than younger persons are (Smit et al., 2014).

Similar ambiguity exists about the differentiating role of education levels. Sheehan (2002) finds higher-educated people are more concerned about their privacy than lower-educated persons, while Smit et al. (2014) find the opposite. Finally, Smit et al. (2014) find a negative correlation between privacy concerns and knowledge about behavioral advertising. While the literature provides no explanation for *why* these differences between groups occur, we intuitively argue that differences in knowledge are key to understanding these differences between groups. Knowledge gap theory describes how the exposure to mass media coverage about an issue (such as privacy) leads to higher levels of knowledge about that specific issue among the people with a higher socio-economic status, in comparison with people with a lower socio-economic status (Tichenor et al., 1970). We want to posit the following: people with higher socio-economic status (i.e. the higher educated) think they understand the threat to their privacy and feel competent to counter it, while the lower-educated people may be aware of an abstract threat to their privacy, but they feel unsure about its specifics and also incapable of countering. Therefore, the lower educated are also more concerned about their privacy. However, we argue that, while the higher educated *think* they understand the threat and feel competent to counter it, in fact, they are wrong. Boerman et al. (2018) indeed show that higher-educated people are more likely to engage in privacy protection behavior, but they generally take ineffective privacy protection measures (e.g. “deleting browser history,” but *not* “using ad blocker”). This suggests that the higher educated neither understand the privacy threat, nor are able to counter it. This also explains why we expect a U-shaped relation between privacy concerns and age groups: the younger “digital immigrants” (as opposed to digital natives) wrongly believe in their privacy protection capabilities, while the older digital immigrants rightly understand their limited privacy protection capabilities. In the discussion section, we will discuss possible mechanisms in more detail.

Predictors of attitudes toward PBT

To our knowledge, attitudes toward PBT have only been comprehensively assessed by Turow et al. (2012), who found that men are a bit more likely to perceive PBT as favorable, older people appear a bit more critical toward PBT than younger people are, and finally, the highest- *and* lowest-educated people hold the most favorable attitudes toward PBT. Again, we could not find an explanation for these differences in the literature. Turow et al. (2012) do stress that, while there are differences between groups, overall, all groups view PBT unfavorably. Some simply perceive PBT more negatively than others. Finally, Smit et al. (2014) find a negative correlation between knowledge (of *online behavioral advertising*; OBA) and attitude toward OBA. Although OBA occurs in the

commercial domain and is, therefore, different from PBT, there is some overlap. This leads to the following hypotheses:

H1a. Women are more likely to be concerned about their privacy than men are.

H2a. Women are more likely to hold unfavorable attitudes toward PBT than men do.

H1b. The youngest and oldest groups of citizens are more likely to be concerned about their privacy than the age groups in between are.

H2b. Older citizens are more likely to hold unfavorable attitudes toward PBT than younger citizens do.

H1c. Lowest and highest educated citizens are more likely to be concerned about their privacy than citizens with an average education are.

H2c. Citizens with a lower education are more likely to hold unfavorable attitudes toward PBT than higher-educated citizens do.

H1d. Citizens with prior knowledge of PBT are less likely to be concerned about their privacy than citizens without prior knowledge of PBT.

H2d. Citizens with prior knowledge of PBT are more likely to hold unfavorable attitudes toward PBT than citizens without prior knowledge of PBT.

The role of internal political efficacy

Political efficacy is usually seen as consisting of two components: external and internal (Wolak, 2017). External efficacy describes individuals' feelings that citizens like themselves have a "voice in politics." Internal efficacy describes individuals' feelings that they themselves are capable of being an active citizen. Someone can believe she is personally capable of being an active citizen (high internal efficacy), but that the political system is filled with selfish and incompetent politicians who are unresponsive to citizens (low external efficacy) (Ostrander et al., 2017; Wolak, 2017: 3). High internal political efficacy is associated with political participation, such as casting a vote (Moeller et al., 2014).

We expect efficacious people to hold unfavorable attitudes toward PBT, as the technique can be seen as diametral to their self-conception as autonomous active citizens (see similar reflections on nudging by Nys and Engelen (2016)). Campaigns using PBT techniques serve citizens with specific, relevant, political information. Efficacious citizens do not need the "help" of political campaigns in deciding what information is relevant to them, as they are capable to browse the *marketplace of ideas* by themselves. For the inefficacious citizen, however, PBT can be very helpful in receiving, processing, and understanding relevant political information. A similar dynamic occurs in the realm of voting advice applications: inefficacious voters are more likely to turn to these applications to gain information about politics (Van de Pol et al., 2014). Moreover, efficacious citizens are likely worried about their personal data, as data enable political campaigns to target them with tailored messages, thereby threatening their efficacy. Non-inefficacious citizens are unlikely to feel the same way: they stand to win efficacy by offering a bit of privacy. This leads to the following hypotheses:

H3a. Efficacious citizens are more likely to be concerned about their privacy than non-efficacious citizens are.

H3b. Efficacious citizens are more likely to hold unfavorable attitudes toward PBT than non-efficacious citizens are.

The change of attitudes toward PBT over time

We study the attitude toward PBT. Attitudes consist of a cognitive component and an affective component (Millar and Tesser, 1986; Moon, 2013). Both components together can lead to a certain behavior (Millar and Tesser, 1989), which makes it important to examine people's attitudes.

How might an attitude guide future behavior in the case of PBT? Consider the following hypothetical, but realistic, scenario: (1) receiving personalized political messages contributes to a feeling of creepiness (affective component) or to a concern about a potential privacy violation (cognitive component); (2) a consequence of this unfavorable attitude can be self-censorship when collecting information about (controversial) standpoints of political parties (behavior) (McDonald and Cranor, 2010).

Information about voters' attitudes toward PBT is scarce. US-based research (Turow et al., 2012) suggests that privacy concerns play a role in shaping negative attitudes toward PBT. This is supported by Smit et al. (2014), who found a negative relation between privacy concerns and attitude toward *commercial* behavioral targeting, and by Schwaig et al. (2013), who found that "general concern for information privacy strongly influences" attitudes towards a "specific information practice" (p. 6). Voters may be concerned about their privacy, since campaigns collect their personal information, and attempts to pseudonymize or anonymize personal data often do not make it impossible to tie pieces of data to individuals (Zuiderveen Borgesius, 2016).

This dynamic is likely to be reciprocal. People initially are unlikely to hold stable attitudes toward PBT because of the novelty of the technique. However, over time, attitudes can become more stable, for instance, as a result of news coverage on the topic or because of direct experience with PBT (Glasman and Albarracin, 2006). Turow et al. (2012) show that Americans hold unfavorable attitudes toward PBT. We expect this negativity toward PBT to hold for the Dutch electorate, since there is no evidence pointing to the contrary. People holding unfavorable attitudes are likely to refer to their privacy concerns as an argument for their unfavorable perception of PBT (Turow et al., 2012). Through the occurrence of attitude congruence bias, where people judge arguments in line with their attitude as more convincing than conflicting arguments (Taber et al., 2009), attitudes will not only become more stable over time, but congruent arguments will become more convincing as well. Since we expect privacy concerns to be an important argument in the shaping of attitude, over time, we expect that attitude toward PBT, in turn and over time, shapes privacy concerns as well. An unfavorable attitude toward PBT, over time, leads to more privacy concerns.

A different scenario is the occurrence of a *positive* reinforcing spiral. A positive reinforcing spiral could lead citizens to not guarding their personal data and to welcome microtargeted messages from political parties, which should become increasingly precise as the campaigns gather more and more data. Such a development could negatively

influence the quality of the public discourse (Gorton, 2016), the ability of journalists to scrutinize political campaigns (Jamieson, 2013), or raise questions about the mandate of the elected politicians (Barocas, 2012). Naturally, the importance of privacy to society (e.g. Reiman, 1995) holds even if citizens themselves do not value their own privacy. A silver lining of a positive spiral is the potential for relevant information sent by campaigns, potentially activating otherwise politically inactive citizens.

As we do not yet have a rationale for the direction of the relation, we have formulated the following research question:

RQ2. How are change in attitude toward PBT and change in the experience of privacy concern related over time?

In sum, together, we expect attitude toward PBT and privacy concerns to form a reinforcing spiral, each, over time, exacerbating the other.

Methods

We use a three-wave panel survey, administered in the Netherlands, between November 2016 and August 2017, by CentERdata (Tilburg University, The Netherlands). There was a national election in the Netherlands during the data-collection period. Wave 1 preceded the election, and the second wave was administered closely after the election. The third wave followed 3 months after. The Netherlands is an interesting case, because during the political campaign people are more likely to receive PBT-messages, and media are more likely to cover the subject.

The sample was drawn from CentERData's LISS panel² and is representative of the Dutch population. Panel members participate in monthly online surveys. The panel is based on a true probability sample of households drawn from the population register. CentERdata carries out a yearly longitudinal survey in the panel, to keep track of changes in a broad range of background variables.

The survey data are part of an overarching project using the same set of panel respondents for eight rounds of data collection. The three waves used in this study are data collection rounds 5, 7, and 8 in the overarching project. As a result, attrition starts after the first wave. Drawing from the pool of participants of wave 1, there were 1193 respondents still participating in wave 5 (79% compared with wave 1),³ which took place in November 2016. In wave 7 (between 15 May 2017 and 20 June 2017), 1031 respondents participated (68%). In wave 8 (in August 2017), 988 respondents participated (66%). We only use data from waves 5, 7, and 8, and therefore, for clarity, refer to those waves as T1, T2, and T3. Furthermore, for our analysis, we rely only on respondents who have completed the surveys at T1, T2, and T3 ($N=879$; 58%). Due to the cooperative nature of the data collection effort, the period between T1 and T2 (6 months) is larger than the period between T2 and T3 (3 months). This may have a detrimental effect on our ability to measure effects between T2 and T3. Potential effects after the 3-month period are likely weaker than potential effects after the 6-month period⁴ (see Appendix 1 for sample descriptives).

Table 1. Descriptive statistics of “attitude towards PBT” over time.

Attitude toward PBT	A	M	SD	Min	Max
T1	.83	2.55	1.59	1	7
T2	.81	2.72	1.64	1	7
T3	.88	2.54	1.54	1	7

PBT: political behavioral targeting; SD: standard deviation.

“Attitude towards PBT” over time (respondents saw only the endpoints written out: 1 = very unfavorable, 7 = very favorable). $N=879$.

Table 2. Descriptive statistics of “privacy concerns” over time.

Privacy concerns	A	M	SD	Min	Max
T1	.93	4.80	1.42	1	7
T2	.92	4.66	1.40	1	7
T3	.94	5.27	1.37	1	7

SD: standard deviation.

“Privacy concerns” over time (respondents saw only the endpoints written out: 1 = totally disagree, 7 = totally agree). $N=879$.

Measures

Attitude toward PBT. Attitude is measured through three items on a 7-point scale: “I do mind if a political party tries to find out my political opinions on the basis of my online surf and search behavior” (T1: $M=2.25$, $SD=1.78$, $\text{min}=1$, $\text{max}=7$), “If I would know a website would share my personal data and online behavior with political parties, I would not visit that website anymore” (T1: $M=2.59$, $SD=1.84$, $\text{min}=1$, $\text{max}=7$), “If I would find out that a website serves me advertisements from political parties based on my personal data, I would be angry” (T1: $M=2.81$, $SD=1.92$, $\text{min}=1$, $\text{max}=7$). Table 1 shows “attitude towards PBT” is a reliable scale. The attitudes are quite unfavorable. Although the between subject mean scores do not seem to vary a lot over time, the within subject standard deviation is .85.

Privacy concerns. Privacy concerns are measured through five items on a 7-point scale: “I am worried that my personal data (such as my online surf and search behavior, name, and location) will be abused by others” (T1: $M=5.04$, $SD=1.55$, $\text{min}=1$, $\text{max}=7$). “When I am online, I get the feeling that others keep track of where I click and what websites I visit” (T1: $M=4.14$, $SD=1.75$, $\text{min}=1$, $\text{max}=7$). “I am afraid that the personal data I share, is not being stored securely” (T1: $M=4.78$, $SD=1.53$, $\text{min}=1$, $\text{max}=7$). “I worry that my personal data on the internet will be passed on to other companies” (T1: $M=4.92$, $SD=1.59$, $\text{min}=1$, $\text{max}=7$). “I worry that my personal data on the internet are seen by people I do not know” (T1: $M=4.85$, $SD=1.64$, $\text{min}=1$, $\text{max}=7$). Table 2 shows fairly high privacy concerns. The within subject standard deviation over time is .78.

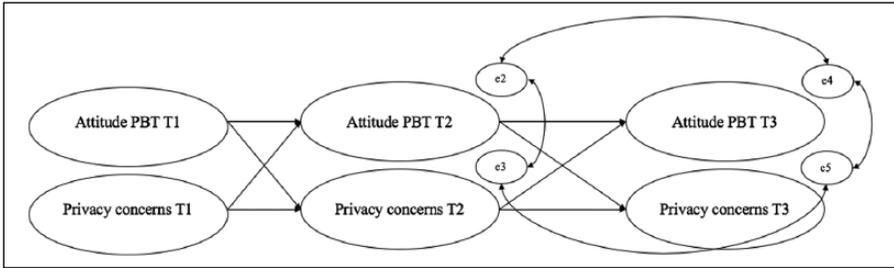


Figure 1. Cross-lagged model attitude toward PBT and privacy concerns over time.

Efficacy. Efficacy is measured with two items, on a 7-point scale: “I know the most important political problems in our country quite well” ($M=4.39$, $SD=1.59$, $\text{min}=1$, $\text{max}=7$), “I am more up to speed with current political affairs than most people in the Netherlands” ($M=3.42$, $SD=1.61$, $\text{min}=1$, $\text{max}=7$). The scale statistics are as follows: $r=.67$; $M=3.91$; $SD=1.46$.

Education levels. Respondents were asked about the highest level of education they have completed. There were six possible subcategories. In line with government data (Statistics Netherlands, 2018), we have recoded these subcategories in “low educated” (elementary school), “middle educated” (different levels of high school and community college), and “high educated” (bachelor’s and master’s degree) (see Appendix 2 for the sample distribution in comparison with the population).

Knowledge of PBT. Knowledge of PBT is measured with one item, explaining that political campaigns can use citizens’ personal data to show them tailored advertisements. Respondents could answer “no” (0) or “yes” (1) to “Were you familiar with the phenomenon, before you enrolled in this study?” The majority (67%) indicated no prior knowledge of PBT. We asked the respondents whom indicated prior knowledge to label three statements true or false to test their knowledge: “Microtargeting requires a lot of personal voter data” (true), “Microtargeting solely takes places on social media” (false), “Microtargeting is illegal in the Netherlands” (false). Only 29% answered all three questions correctly, 51% answered 2 questions correctly, 17% answered 1 question correctly, and 2% gave no correct answers.

Analytical strategy. First, we examine the characteristics of the people who are concerned about their privacy, and those of the people holding negative attitudes toward PBT at one point in time (T1). Then, using a second model, we focus on the reciprocal relation between privacy concerns and attitude toward PBT and investigate a potentially negative reinforcing spiral over time. Since we incorporate stability coefficients in this second model, we do control for the *previous* values of the same variable (Adachi and Willoughby, 2015). After all, often, the best way to predict a future value is to look at the value at T1. By taking these previous values in account, we track within-respondent changes over time *and* distill the effect of other variables over time (see Figure 1 for a

Table 3. OLS regression predicting privacy concern at T1.

Privacy concerns (T1)	B	SE B	β	t	p
Age (centered)	.01	.003	.10	2.61	.001
Age (centered, squared)	-.00	.00	-.08	-2.18	.03
Gender (0=F, 1=M)	-.09	.10	-.03	-.97	.33
Education (1-7)	-.11	.09	-.05	-1.33	.19
Knowledge of PBT (0=No, 1=Yes)	.15	.11	.05	1.37	.17
Efficacy (1-7)	.05	.04	.05	1.44	.15
Constant	4.95	.21		23.13	<.001

PBT: political behavioral targeting; SE: standard error; OLS: ordinary least squares.
 OLS regression predicting privacy concerns at T1. $R^2 = .03$. $N = 874$.

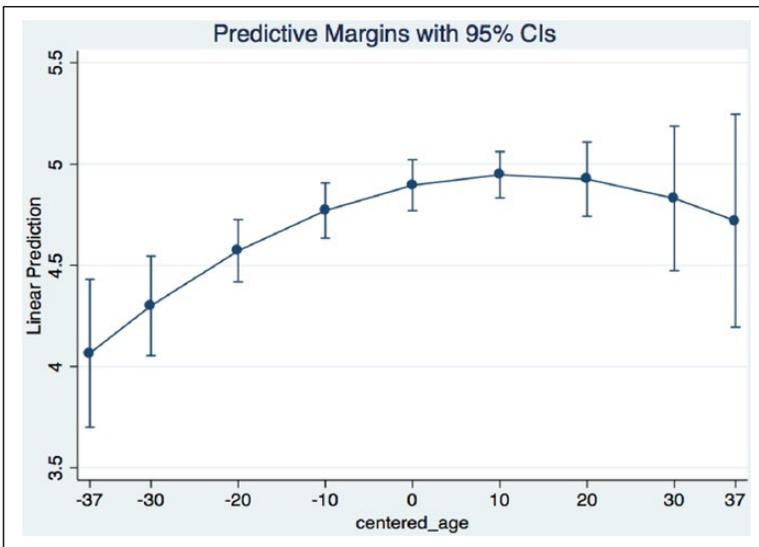


Figure 2. Margins plot showing relation between privacy concerns and age groups (mean age = 56 years old).

schematic diagram of the cross-lagged model). A two-step approach, using separate models, is needed to overcome an insufficient model fit. This way, we can provide a deeper understanding of the phenomenon by taking background variables into account.

Results

As Table 3 shows, age is the only significant predictor of privacy concerns. However, as the low R^2 (.03) indicates, none of these variables add much to our understanding of the privacy-concerned citizen. Figure 2 shows a non-linear relation between age and privacy concerns. The expected U shape, however, was not found. Rather, the opposite appears

Table 4. OLS regression predicting attitude toward PBT at T1.

Attitude toward PBT (T1)	B	SE B	β	t	p
Age	-.03	.003	-.31	-9.50	<.001
Gender (0=F, 1=M)	.30	.11	.09	2.84	.01
Education (1-7)	.12	.09	.04	1.29	.20
Knowledge of PBT (0=No, 1=Yes)	.40	.11	.12	3.61	<.001
Efficacy (1-7)	.04	.04	.03	0.98	.33
Constant	3.59	.29		12.23	<.001

PBT: political behavioral targeting; SE: standard error; OLS: ordinary least squares.
 OLS regression predicting attitude toward PBT. $R^2 = .15$. $N = 874$.

true: the youngest age group is the least concerned about their privacy. This concern increases with age, but stops—and starts trending downward—at around 65 years. Looking at Table 3, we can see that indeed men appear less worried about their privacy (H1a), but hypotheses 1b, 1c, 1d, and 3a are not supported.

Table 4 shows that age is the most important predictor of citizens' attitude toward PBT. Older people are more likely to hold unfavorable attitudes. Women are more likely to hold unfavorable attitudes toward PBT than men do. Having prior knowledge of PBT is positively related to attitude toward PBT. This was expected in H2a, H2b, and H2d. Education level or the level of efficacy, finally, does not seem to be related to attitude toward PBT (contrary to H2c, H3b). As the explained variance ($R^2 = .15$) shows, we are much better able to explain the attitude toward PBT than we were able to explain privacy concerns.

Before we estimate a structural equation model to study the relationship between privacy concerns and attitude toward PBT over time, we first take a closer look at both variables at T1. Figure 3 shows the correlation between privacy concerns and attitude toward PBT ($r = -.32$) and the distribution of both variables at T1. As expected, being more concerned about one's privacy is related to a less positive attitude toward PBT. But we also see that at the first point in time, a relatively large number of respondents already take on the most extreme values for both privacy concerns (very concerned) as well as attitude toward PBT (very unfavorable). This implies a ceiling effect where, over time, people cannot take on even more extreme values. As a result, it is possible that our following model underestimates the relation between attitude toward PBT and privacy concerns.

Estimating the cross-lagged model (see Figure 1), we find that the cross-lagged model fits the data rather well: χ^2 (2 df) = 5.37, $p = .07$; root mean square error approximation (RMSEA) = .04, 90% confidence interval (CI) = [.00 to .09]; comparative fit index (CFI) = .998.⁵ Figure 4 only shows the significant paths. Indeed, we find a reciprocal relation between attitude toward PBT and privacy concerns between T1 and T2. The hypothesized reciprocity disappears between change in privacy concerns at T2 and attitude toward PBT at T3 ($B = -.06$; $SD = .04$; $z = -1.65$; $p = .10$; 95% CI = [-.13 to .01]).⁶ There is, however, still a significant influence of change in attitude toward PBT at T2 on change in privacy concerns at T3.

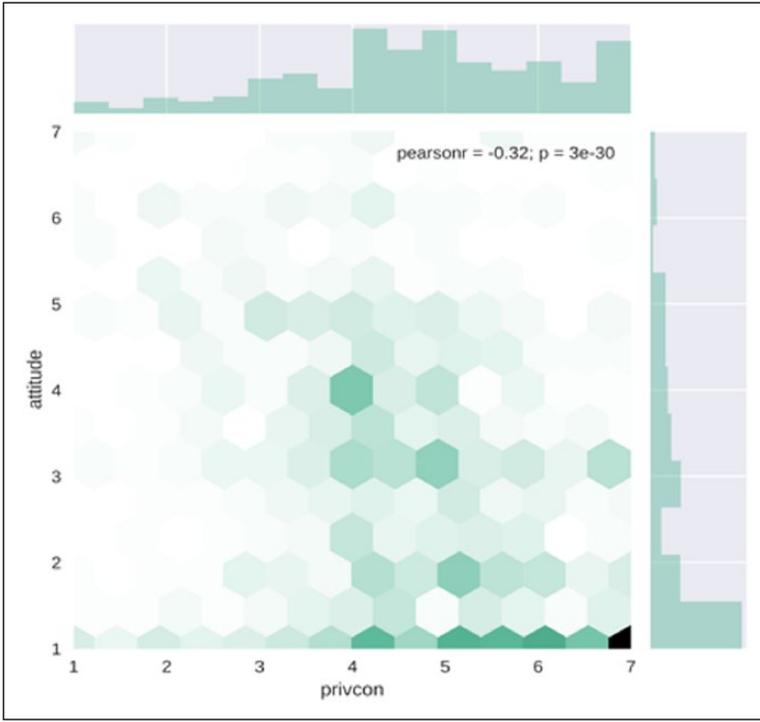


Figure 3. Hex plot showing correlation and distribution of privacy concerns and attitude toward PBT at T1.

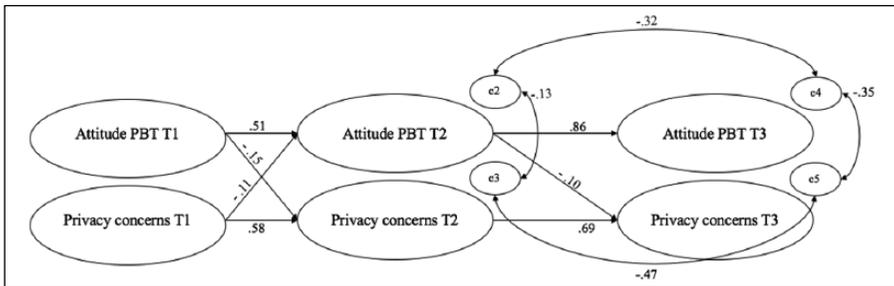


Figure 4. Significant coefficients cross-lagged model.

Discussion and conclusion

In this article, we set out to explore the reciprocal relation between privacy concerns and attitude toward PBT over time, and we examined the role of demographics therein. We showed a reciprocal relation between both variables over time, but the effect appears to wash out over time. Remarkably, age, gender, and education together fall

short in explaining people's experience of privacy concerns (see Table 3). Even when internal political efficacy and prior knowledge of PBT are added to the model, the explained variance remains very low ($R^2 = .03$). We can only conclude that younger age groups, in general, are less concerned about their privacy. Education level does not seem to be a significant predictor of privacy concerns. This may suggest that privacy concerns are not limited to a specific subset of society (e.g. the educated elite) but are rather a society-wide phenomenon. It could also indicate an "experience gap" in the sense that digital natives feel more competent in countering the threats to their privacy. A divide between "digital natives" and "digital immigrants" is possible. Differences in perceptions and experiences between both groups have been found in online trust (Hoffmann et al., 2014). Finally, our findings are in line with earlier findings by Baruh et al. (2017), who have shown women are generally more concerned about their privacy than men are.

Looking at the relationship between demographics and attitudes toward PBT (see Table 4), our results show that people with prior knowledge of PBT hold more favorable attitudes toward PBT. This finding contrasts with Smit et al. (2014), who found a negative correlation between knowledge and OBT. Furthermore, only 33% of the sample claimed to be aware of PBT before survey participation. Of those 33%, a bit less than a third answered all three follow-up knowledge questions correctly. This makes it possible that a large chunk of the people who indicated prior knowledge of PBT had no deep understanding of the phenomenon. What stands out, as was the case with privacy concerns, is that age is an important indicator for citizens' attitude toward PBT. The "digital divide" we may have seen in relation to privacy concerns seems to be manifesting itself here as well.

Now that we better understand which demographic variables relate to privacy concerns and attitudes toward PBT at T1, we can discuss the cross-lagged model. We indeed find some evidence for a reinforcing spiral: changes in privacy concerns lead to changes in attitude toward PBT, and vice versa, over time. Between T1 and T2, we find a clear reciprocal relation. Between T2 and T3, however, the reciprocity does not hold for both variables. Change in attitude toward PBT at T2 *does* lead to change in privacy concerns at T3, but change in privacy concerns at T2 *does not* significantly lead to change in attitude toward PBT at T3. This makes sense because the time period between T2 and T3 was 3 months shorter than the time period between T1 and T2. Furthermore, there was an election between T1 and T2, so we would expect a stronger effect during the election period. After all, during the election, people are more likely to have actually experienced or heard about PBT. Concluding, we have seen a negative reciprocal relation, but the effect is (1) limited to a longer period of time, which gives people more time to change their minds; (2) likely strengthened by a time period in which there is media attention for PBT and in which people can actually encounter PBT messages from political campaigns; and (3) potentially underestimated due to the earlier mentioned ceiling effect (see Figure 3).

This is the first time empirical evidence has been presented for detrimental consequences of PBT on voter attitude and privacy concerns. For example, Tufekci (2014) discusses the information asymmetry between political campaigns and the individual voter. Tufekci likens this asymmetry with the "opposite of the panopticon" (p. 9), where

surveillance is implicit instead of explicit. According to Tufekci, this implicit surveillance is needed, because, contrary to the “original” panopticon, in a democratic society, the information gatherer does not surveille prisoners, but citizens. And these citizens “may be upset about surveillance and loss of privacy—and take action against it” (p. 9). Our model supports Tufekci’s observation: it shows how using PBT techniques on people who are already concerned about their privacy is a bad idea (see Figure 4).

Our findings also warrant concern about a loss of autonomy voters may experience (e.g. Anderson, 2013). As citizens are quite concerned about their privacy, the process of independently forming political opinions is being jeopardized. After all, citizens’ independence is on the line when third parties hold vast amounts of personal data that would allow them to arbitrarily interfere in people’s lives (see, for example, Pettit, 2017; Tene and Polonetsky, 2013). When citizens, in addition to this, are increasingly concerned about their privacy, their *feeling of autonomy* suffers. Concerned citizens may fear sanctions following data analyses from third parties, which show they are likely to deviate from the popular opinion. Or they may fear that their search behavior, in the near future, reveals something about themselves that might be used against them. As a result, autonomous deliberation becomes riskier. Therefore, there is less opportunity for equal participation. From a republican perspective, this “privacy-concerned citizen” finds herself in a disadvantaged position, as she fears the consequences that may follow the data trail showing her deviating from the popular opinion (see Noelle-Neumann, 1974; Pettit, 2017, but also Scheufele and Moy, 2000). From a liberal perspective, democracy benefits from a diverse marketplace of ideas. While there may still be a diverse range of ideas on this marketplace, the privacy-concerned citizen will not hear them, as she self-censors her behavior to avoid penalization.

Political campaigns should be transparent about their influencing techniques. Explaining the targeted audience that they receive a tailored message may help limit the feeling of manipulation. Explaining how they take care of citizens’ privacy may positively address privacy concerns. Taken together, our findings show that the potential for undesirable voter behavior (e.g. inability to deliberate autonomously, chilling effects, voter mistrust; Anderson, 2013; McDonald and Cranor, 2010; Turow et al., 2012) is very real.

Future research should delve deeper into the relationship between PBT and privacy concerns. It would be interesting to examine differences between the lower-educated and the higher-educated, over time, through the lens of knowledge gap theory (Tichenor et al., 1970). PBT messages could be especially useful for the lower-educated, since tailored messages could inform them on relevant policy issues. As a result, we expect that for these groups, privacy concerns play a minor role, since the PBT messages are useful for them. This is in line with privacy calculus (Bol et al., 2018; Dinev and Hart, 2006). However, it can be questioned whether people can really oversee PBT’s usefulness to them personally. An interesting question for future research can also be whether privacy concerns and attitude toward PBT have an impact on political efficacy. Although internal political efficacy can be considered a stable variable (e.g. Schneider et al., 2014), over time, a relation is not unimaginable. Finally, as data gathering and microtargeting do not happen in the political domain alone, future research should compare attitudes toward PBT and privacy concerns in different realms.

Acknowledgements

This article is written as part of the Personalised Communication Project of the University of Amsterdam.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This project is funded by the University of Amsterdam.

Notes

1. Chilling effects are just a potential detrimental consequence, next to, for example, political cynicism or voter manipulation.
2. A detailed description of the sample is given here (PDF): https://www.lissdata.nl/sites/default/files/bestanden/Sample%20and%20Recruitment_1.pdf.
3. A total of 1508 complete respondents in wave 1.
4. Because participants answered attitude and privacy concern questions multiple times, a learning effect could occur. There also is a possibility that people who dropped out of the panel, did so because of privacy concerns. Even though this potentially weakens the quality of our data, we believe that these two risks are common to panel research and unlikely to be problematic because our intervals were relatively long.
5. We also estimated the cross-lagged model with gender, education, year of birth, and efficacy as exogenous variables, but the fit indices indicated a slightly worse fit than the model we present, χ^2 (14 df) = 76.51, $p = .000$; RMSEA = .07, 90% CI = [.06 to .09]; CFI = .969, and so we decided to model these variables separately.
6. A fixed effects model, performed as a robustness check, however, not only shows PBT attitude negatively affects privacy concerns over time ($b = -.18$, $SE = .02$, $t = -8.52$, $p < .001$, 95% CI = [-.23 to -.14]) but also the other way around, privacy concerns negatively influence PBT attitude over time ($b = -.21$, $SE = .03$, $t = -8.52$, $p < .001$, 95% CI = [-.26 to -.17]).

ORCID iD

Tom Dobber  <https://orcid.org/0000-0002-6657-4037>

References

- Adachi P and Willoughby T (2015) Interpreting effect sizes when controlling for stability effects in longitudinal autoregressive models: implications for psychological science. *European Journal of Developmental Psychology* 12(1): 116–128.
- Anderson J (2013) Autonomy. In: LaFollette H (ed.) *The International Encyclopedia of Ethics*. Hoboken, NJ: Blackwell Publishing Ltd, pp. 1–17.
- Anstead N (2017) Data-driven campaigning in the 2015 UK general election. *International Journal of Press/Politics* 22: 294–313.
- Barocas S (2012) The price of precision: voter microtargeting and its potential harms to the democratic process. In: *Proceedings of the first edition workshop on politics, elections and data (PLEAD'12)*, Maui, HI, 29 October–2 November, pp. 31–36. New York: ACM.
- Baruh L, Secinti E and Cemalcilar Z (2017) Online privacy concerns and privacy management: a meta-analytical review. *Journal of Communication* 67(1): 26–53.
- Bennett CJ (2015) Trends in voter surveillance in Western societies: privacy intrusions and democratic implications. *Surveillance and Society* 13(3): 370–384.

- Bennett CJ (2016) Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America? *International Data Privacy Law* 6(4): 261–275.
- Bimber B (2014) Digital media in the Obama campaigns of 2008 and 2012: adaptation to the personalized political communication environment. *Journal of Information Technology & Politics* 11(2): 130–150.
- Boerman SC, Kruijemeier S and Zuiderveen Borgesius FJ (2018) Blocking ads and removing cookies: a longitudinal study examining online privacy protection behavior. In: *Annual conference of the American Academy of Advertising (AAA) 2018*, Marriott Downtown, NY, 22–25 March.
- Bol N, Dienlin T, Kruijemeier S, et al. (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.
- Broockman DE and Green DP (2012) Do online advertisements increase political candidates' name recognition or favorability? Evidence from randomized field experiments. *Political Behavior* 36(2): 263–289.
- Dawes S (2014) Press freedom, privacy and the public sphere. *Journalism Studies* 15(1): 17–32.
- Dinev T and Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17(1): 61–80.
- Dobber T, Trilling D, Helberger N, et al. (2017) Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques. *Internet Policy Review* 6(4): 1–25.
- Endres K (2016) The accuracy of microtargeted policy positions. *PS: Political Science and Politics* 49(4): 771–774.
- Gavison R (1980) Privacy and the limits of law. *The Yale Law Journal* 89(3): 421–471.
- Glasman LR and Albarracín D (2006) Forming attitudes that predict future behavior: a meta-analysis of the attitude behavior relation. *Psychological Bulletin* 132(5): 778–822.
- Gorton WA (2016) Manipulating citizens: how political campaigns' use of behavioral social science harms democracy. *New Political Science* 38(1): 61–80.
- Hersh ED (2015) *Hacking the Electorate: How Campaigns Perceive Voters*. New York: Cambridge University Press.
- Hersh ED and Schaffner BF (2013) Targeted campaign appeals and the value of ambiguity. *Journal of Politics* 75(2): 520–534
- Hoffmann CP, Lutz C and Meckel M (2014) Digital natives or digital immigrants? The impact of user characteristics on online trust. *Journal of Management Information Systems* 31(3): 138–171.
- Hoofnagle C, King J, Li S, et al. (2010) How different are young adults from older adults when it comes to information privacy attitudes and policies? Research Report. Annenberg School for Communication, University of Pennsylvania, Philadelphia, PA, 14 April.
- Howard PN (2006) *New Media Campaigns and the Managed Citizen*. Cambridge: Cambridge University Press.
- Jamieson KH (2013) Messages, micro-targeting, and new media technologies. *Forum* 11(3): 429–435.
- Kreiss D (2012) *Taking Our Country Back: The Crafting of Networked Politics from Howard Dean to Barack Obama*. New York: Oxford University Press.
- Kreiss D (2016) *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy*. New York: Oxford University Press.
- McDonald AM and Cranor LF (2010) Beliefs and behaviors: internet users' understanding of behavioral advertising. In: *TPRC2010*. Available at: <https://ssrn.com/abstract=1989092>
- Marder B, Joinson A, Shankar A, et al. (2016) The extended “chilling” effect of Facebook: the cold reality of ubiquitous social networking. *Computers in Human Behavior* 60: 582–592.

- Millar MG and Tesser A (1986) Effects of affective and cognitive focus on the attitude-behavior relation. *Journal of Personality and Social Psychology* 51(2): 270–276.
- Millar MG and Tesser A (1989) The effects of affective-cognitive consistency and thought on the attitude-behavior relation. *Journal of Experimental Social Psychology* 25(2): 189–202.
- Moeller J, De Vreese C, Esser F, et al. (2014) Pathway to political participation. *American Behavioral Scientist* 58(5): 689–700.
- Moon SJ (2013) Attention, attitude, and behavior. *Communication Research* 40(5): 698–719.
- Nickerson D and Rogers T (2014) Political campaigns and big data. *Journal of Economic Perspectives* 28(2): 51–74.
- Nielsen RK (2012) *Ground Wars: Personalized Communication in Political Campaigns*. Princeton, NJ: Princeton University Press.
- Noelle-Neumann E (1974) The spiral of silence a theory of public opinion. *Journal of Communication* 24: 43–51.
- Nys TR and Engelen B (2016) Judging nudging: answering the manipulation objection. *Political Studies* 65(1): 199–214.
- Ostrander JA, Lane S, McClendon J, et al. (2017) Collective power to create political change: increasing the political efficacy and engagement of social workers. *Journal of Policy Practice* 16(3): 261–275.
- Panagopoulos C (2016) All about that base: changing campaign strategies in U.S. presidential elections. *Party Politics* 22(2): 179–190.
- Penney JW (2016) Chilling effects: online surveillance and Wikipedia use. *Berkeley Technology Law Journal* 31(1): 119–174.
- Pettit P (2017) Is Facebook making us less free? *iai News*. Available at: <https://iainews.iai.tv/articles/the-big-brotherhood-of-digital-giants-is-taking-away-our-freedom-auid-884> (accessed 2 February 2018).
- Reiman JH (1995) Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Computer & High Technology Law Journal* 11(1): 27–44.
- Richards NM (2015) *Intellectual Privacy*. New York: Oxford University Press.
- Scheufele DA and Moy P (2000) Twenty-five years of the spiral of silence: a conceptual review and empirical outlook. *International Journal of Public Opinion Research* 12(1): 3–28.
- Schneider FM, Otto L, Alings D, et al. (2014) Measuring traits and states in public opinion research: a latent state–trait analysis of political efficacy. *International Journal of Public Opinion Research* 26(2): 202–223.
- Schwaig KS, Segars AH, Grover V, et al. (2013) A model of consumers' perceptions of the invasion of information privacy. *Information and Management* 50(1): 1–12.
- Sheehan KB (2002) Toward a typology of internet users and online privacy concerns. *Information Society* 18(1): 21–32.
- Smit EG, Van Noort G and Voorveld HAM (2014) Understanding online behavioural advertising: user knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior* 32: 15–22.
- Statistics Netherlands (2018) Population; highest completed level of education and type of education. Available at: <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/82816ned/table?dl=8083> (accessed 1 October 2018).
- Taber CS, Cann D and Kucsova S (2009) The motivated processing of political arguments. *Political Behavior* 31(2): 137–155.
- Tene O (2011) Privacy: the new generations. *International Data Privacy Law* 1(1): 15–27.

- Tene O and Polonetsky J (2013) Big data for all: privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property* 11(5): 240–272.
- Tichenor PJ, Donohue GA and Olien CN (1970) Mass media flow and differential growth in knowledge. *The Public Opinion Quarterly* 34(2): 159–170.
- Tufekci Z (2014) Engineering the public: big data, surveillance and computational politics. *First Monday* 19(7): 1–14.
- Turow J, Delli Carpini MX, Draper NA, et al. (2012) *Americans Roundly Reject Tailored Political Advertising*. Philadelphia, PA: Annenberg School for Communication, University of Pennsylvania.
- Turow J, Hennessy M, Draper NA, et al. (2018) *Divided We Feel: Partisan Politics Drive Americans' Emotions Regarding Surveillance of Low-Income Populations*. Philadelphia, PA: Annenberg School for Communication, University of Pennsylvania.
- Van de Pol J, Holleman B, Kamoen N, et al. (2014) Beyond young, highly educated males: a typology of VAA users. *Journal of Information Technology & Politics* 11(4): 397–411.
- Wolak J (2017) Feelings of political efficacy in the fifty states. *Political Behavior* 40: 763–784.
- Youyou W, Kosinski M and Stillwell D (2015) Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences* 112(4): 1036–1040.
- Zuiderveen Borgesius FJ (2016) Singling out people without knowing their names-behavioural targeting, pseudonymous data, and the new data protection regulation. *Computer Law and Security Review* 32(2): 256–271.
- Zuiderveen Borgesius FJ, Möller J, Kruike-meier S, et al. (2018) Online political microtargeting: promises and threats for democracy. *Utrecht Law Review* 14(1): 82–96.

Author biographies

Tom Dobber is a PhD candidate at the University of Amsterdam and a member of the Department of Political Communication and Journalism at the Amsterdam School of Communication Research.

Damian Trilling is an assistant professor at the University of Amsterdam and a member of the Department of Political Communication and Journalism at the Amsterdam School of Communication Research.

Natali Helberger is a professor in Information Law at the University of Amsterdam, at the Institute for Information Law.

Claes de Vreese is a professor of Political Communication at the University of Amsterdam, chair of the Department of Political Communication and Journalism at the Amsterdam School of Communication Research.

Appendix 1

Sample descriptives

Appendix 1 shows that the mean age of the sample is higher than the population mean (Statistics Netherlands, 2017). This is because our sample consists of people aged 18 years or older. The men/women distribution in our sample is comparable with the population mean.

	T1	μ
Age	56.4	41.5
Gender (men)	51.8%	49.57%

Descriptive statistics sample.

Appendix 2

Education level

Appendix 2 shows the distribution on education levels is similar to the population mean (Statistics Netherlands, 2018).

Education levels	T1 (%)	T2 (%)	μ (%)
Elementary school	7	7	10
High school/community college	58	58	60
Bachelor's degree	24	24	19
Master's degree or higher	12	12	11

Descriptive statistics sample. Numbers may not add up to 100 due to rounding.