



## UvA-DARE (Digital Academic Repository)

### Data & Democracy

*Political microtargeting: A threat to electoral integrity?*

Dobber, T.

#### Publication date

2020

#### Document Version

Other version

#### License

Other

[Link to publication](#)

#### Citation for published version (APA):

Dobber, T. (2020). *Data & Democracy: Political microtargeting: A threat to electoral integrity?*.

#### 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.

---

# Chapter 3

Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns<sup>8</sup>

---

<sup>8</sup> This chapter is published as: Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. (2018). Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns. *New Media & Society*, 21, 1–20. <https://doi.org/10.1177/1461444818813372>

## **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.

## 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 US (e.g. Kreiss, 2016; Hersh, 2015; 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 (Bennet, 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 towards the use of PBT-techniques by political campaigns. This process is likely reciprocal: A more unfavorable attitude towards PBT might also lead to more privacy concerns. Together, privacy concerns and attitude towards 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 & Cranor, 2010; p. 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; p. 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, Delli Carpini, Draper, & Williams, 2012), and threaten voters’ intellectual privacy (see Richards, 2015). Moreover, demographics may play a role in predicting privacy concerns or attitudes towards PBT.

We look at the relationship between demographics on the one hand, and privacy concerns and attitudes towards 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, 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 paper. However, we have seen evidence of chilling effects following online behavioral advertising (McDonald & 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 US 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, p. 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, towards 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' 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. Turov 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; p. 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, e.g., Tene & Polonetsky, 2013; Pettit, 2018). 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 & 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, p. 455) 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 judgement (Dawes, 2014) and privacy concerns threaten the experience of such political privacy.

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, Secinti, & Cemalcilar, 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, Kruikemeier, and Zuiderveen Borgesius (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 towards PBT**

To our knowledge, attitudes towards 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 towards PBT than younger people are, and finally, the highest and lowest-educated people hold the most favorable attitudes towards 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 towards 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 towards 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 towards 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 towards 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 towards 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 to be 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) (Wolak, 2017; p. 3; Ostrander et al., 2017). High internal political efficacy is associated with political participation, such as casting a vote (Moeller, De Vreese, Esser, & Kunz, 2014).

We expect efficacious people to hold unfavorable attitudes towards PBT, as the technique can be seen as diametral to their self-conception as autonomous active citizens (see similar reflections on nudging by Nys & 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, Holleman, Kamoen, Krouwel, & de Vreese, 2014). Moreover, efficacious citizens are likely worried about their personal data, as data enables political campaigns to target them with tailored messages, thereby threatening their efficacy. Non-efficacious 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 towards PBT than non-efficacious citizens are.

### **The change of attitudes toward PBT over time**

We study the attitude toward political behavioral targeting (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 & Cranor, 2010).

Information about voters’ attitudes towards PBT is scarce. US-based research (Turow et al., 2012) suggests that privacy concerns play a role in shaping negative attitudes towards PBT. This is supported by Smit, Van Noort, and Voorveld (2014), who

found a negative relation between privacy concerns and attitude towards commercial behavioral targeting, and by Schwaig, Segars, Grover, and Fiedler (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 towards 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 towards PBT. We expect this negativity towards 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 towards PBT, in turn and over time, shapes privacy concerns as well. An unfavorable attitude towards 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 towards PBT and change in the experience of privacy concern related over time?

In sum, together, we expect attitude towards 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 one preceded the election, the second wave was administered closely after the election. The third wave followed three 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 panel, 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 one, there were 1193 respondents still participating in wave 5 (79% compared with wave one), 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, 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 period. See appendix A for sample descriptives.

## Measures

Attitude towards 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:  $M=2.25$ ,  $SD=1.78$ ,  $\min=1$ ,  $\max=7$ ), '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:  $M=2.59$ ,  $SD=1.84$ ,  $\min=1$ ,  $\max=7$ ), 'If I would find out that a website serves me advertisements from political parties based on my personal data, I would be angry' (T1:  $M=2.81$ ,  $SD=1.92$ ,  $\min=1$ ,  $\max=7$ ). Table 3.1 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.

**Table 3.1** - Descriptive statistics of 'attitude toward 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

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

### *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:  $M=5.04$ ,  $SD=1.55$ , min=1, max=7). 'When I am online, I get the feeling that others keep track of where I click and what websites I visit' (T1:  $M=4.14$ ,  $SD=1.75$ , min=1, max=7). I am afraid that the personal data I share, is not being stored securely' (T1:  $M=4.78$ ,  $SD=1.53$ , min=1, max=7). I worry that my personal data on the internet will be passed on to other companies' (T1:  $M=4.92$ ,  $SD=1.59$ , min=1, max=7). 'I worry that my personal data on the internet are seen by people I do not know' (T1:  $M=4.85$ ,  $SD=1.64$ , min=1, max=7). Table 3.2 shows fairly high privacy concerns. The within subject standard deviation over time is .78.

**Table 3.2** - 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

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

### *Efficacy*

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

### *Education levels*

Respondents were asked about the highest level of education they have completed. There were six possible subcategories. In line with government data (Rijksoverheid, 2017), we have recoded these subcategories in either '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 B 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 towards PBT at one point in time (T1). Then, using a second model, we focus on the reciprocal relation between privacy concerns and attitude towards 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 T-1. 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 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.

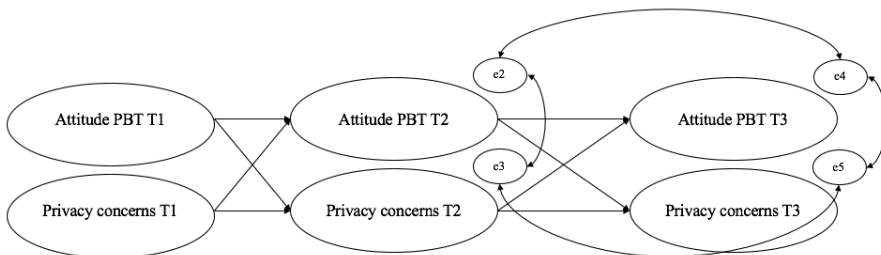


Figure 1 - Cross-lagged model attitude toward PBT and privacy concerns over time.

**Table 3.3** - OLS regression predicting privacy concern at T1.

Privacy concerns (T1)	<i>B</i>	<i>SE B</i>	$\beta$	<i>t</i>	<i>p</i>
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

$R^2=.03$ .  $N=874$ .

## Results

As Table 3.3 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 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 3.3, we can see that indeed men appear less worried about their privacy (H1a), but hypotheses 1b, 1c, 1d, 3a are not supported.

Table 3.4 shows that age is the most important predictor of citizens' attitude towards PBT. Older people are more likely to hold unfavorable attitudes. Women are more likely to hold unfavorable attitudes towards PBT than men do. Having prior knowledge of PBT is positively related to attitude towards PBT. This was expected in H2a, H2b, H2d. Education level or the level of efficacy, finally, do not seem to be related to attitude towards PBT (contrary to H2c, H3b). As the explained variance ( $R^2=.15$ ) shows, we are much better able to explain the attitude towards PBT than we were able to explain privacy concerns.

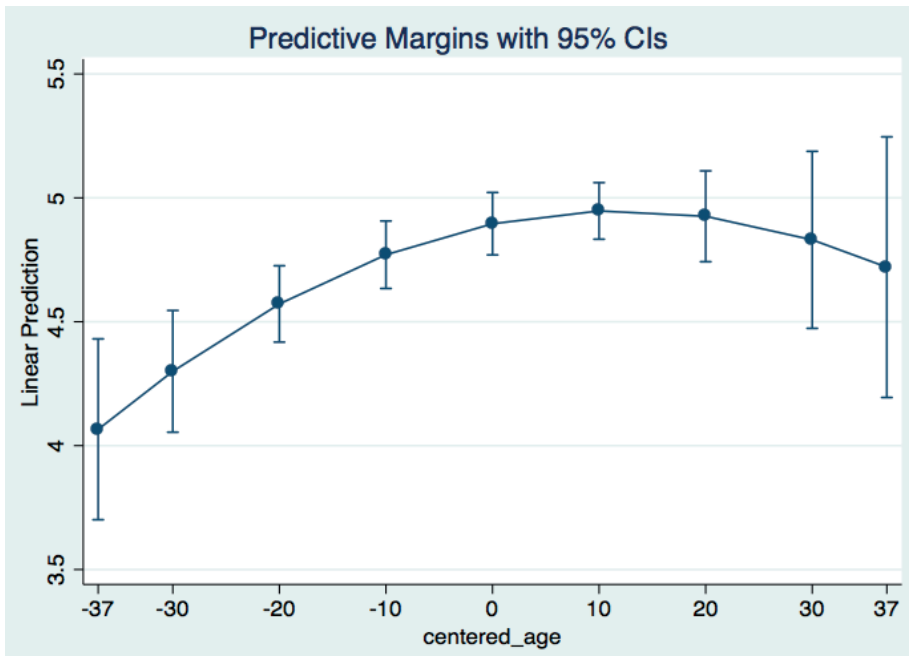
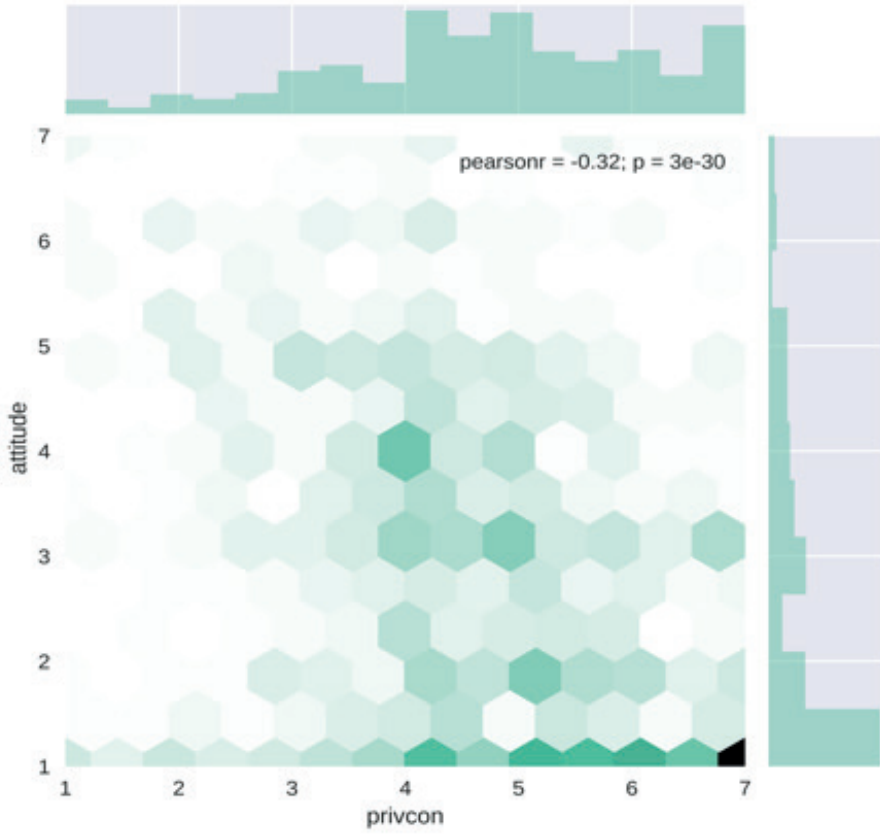


Figure 2 - Margins plot showing relation between privacy concerns and age groups (mean age=56 years old).

Table 3.4 - OLS regression predicting attitude towards PBT at T1.

Attitude towards PBT (T1)	<i>B</i>	<i>SE B</i>	$\beta$	<i>t</i>	<i>p</i>
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

OLS regression predicting attitude towards PBT.  $R^2=.15$ .  $N=874$ .



3

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

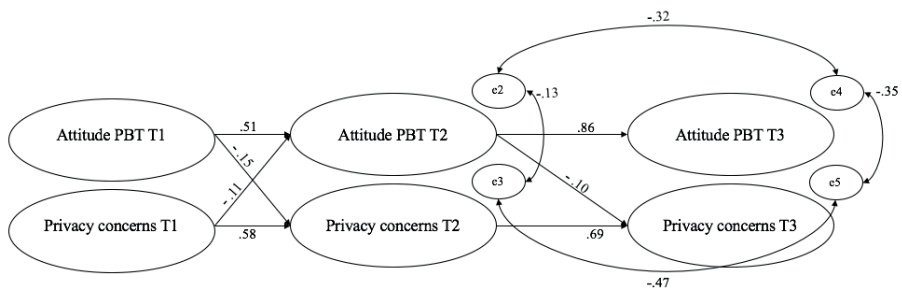


Figure 4 - Significant coefficients cross-lagged model.



Before we estimate a Structural Equation Model to study the relationship between privacy concerns and attitude towards PBT over time, we first take a closer look at both variables at T1. Figure 3 shows the correlation between privacy concerns and attitude towards 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 towards 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 towards 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 towards PBT and privacy concerns.

Estimating the cross-lagged model (see Figure 1), we find that the cross-lagged model fits the data rather well:  $\chi^2$  (2 df) = 5.37,  $p=.07$ ; RMSEA=.04, 90% CI[.00-.09]; CFI=.998). Figure 4 only shows the significant paths. Indeed, we find a reciprocal relation between attitude towards PBT and privacy concerns between T1 and T2. The hypothesized reciprocity disappears between change in privacy concerns at T2 and attitude towards PBT at T3 ( $B=-.06$ ;  $SD=.04$ ;  $z=-1.65$ ;  $p=.10$ ; 95% CI[-.13-.01]). There is, however, still a significant influence of change in attitude towards PBT at T2 on change in privacy concerns at T3.

## Discussion and conclusion

In this paper, we set out to explore the reciprocal relation between privacy concerns and attitude towards 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 3.3). 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 towards PBT (see Table 3.4), our results show that people with prior knowledge of PBT hold more favorable attitudes towards 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 towards 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 towards 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 towards 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 towards 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 towards PBT at T3. This makes sense, because the time period between T2 and T3 was three 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 surveil 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, e.g. Tene & Polonetsky, 2013; Pettit, 2018). 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 Pettit, 2018; and Noelle-Neumann, 1974; but also Scheufele & 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; McDonald & Cranor, 2010; Turow et al., 2012; Anderson, 2013) 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 (Dinev and Hart, 2006; Bol et al., 2018). 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 towards 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 does not happen in the political domain alone, future research should compare attitudes towards PBT and privacy concerns in different realms.