COGITATIO

Media and Communication (ISSN: 2183–2439)
2021, Volume 9, Issue 4, Pages 158–169
https://doi.org/10.17645/mac.v9i4.4085

Article

Political Microtargeting and Online Privacy: A Theoretical Approach to Understanding Users' Privacy Behaviors

Johanna Schäwel *, Regine Frener and Sabine Trepte

Department of Communication Science: Media Psychology, University of Hohenheim, Germany;
E-Mails: johanna.schaewel@uni-hohenheim.de (J.S.), regine.frener@uni-hohenheim.de (R.F.),
sabine.trepte@uni-hohenheim.de (S.T.)

* Corresponding author

Submitted: 29 January 2021 | Accepted: 17 August 2021 | Published: 18 November 2021

Abstract
Social media allow political parties to conduct political behavioral targeting in order to address and persuade specific groups of users and potential voters. This has been criticized: Most social media users do not know about these microtargeting strategies, and the majority of people who are aware of targeted political advertising say that it is not acceptable. This intrusion on personal privacy is viewed as problematic by users and activists alike. The overarching goal of this article is to elaborate on social media users' privacy perceptions and potential regulating behaviors in the face of political microtargeting. This work is theoretical in nature. We first review theoretical and empirical research in the field of political microtargeting and online privacy. We then analyze how privacy is experienced by social media users during political microtargeting. Building on our theoretical analysis, we finally suggest clear-cut propositions for how political microtargeting can be researched while considering users' privacy needs on the one hand and relevant political outcomes on the other.

Keywords
online privacy; political microtargeting; social media affordances; social media privacy model

Issue
This article is part of the issue "Algorithmic Systems in the Digital Society" edited by Sanne Kruikemeier (University of Amsterdam, The Netherlands), Sophie Boerman (University of Amsterdam, The Netherlands) and Nadine Bol (Tilburg University, The Netherlands).

1. Introduction

Political microtargeting can be regarded as a pivotal tool amongst the different campaign instruments that exist. Oftentimes, microtargeting takes place on social media (Papakyriakopoulos et al., 2017). Consequently, the vast majority of users report having encountered political ads on social media (Media Authority of North Rhine-Westphalia [MANRW], 2019). However, despite its importance, political microtargeting was not extensively discussed until 2015, when a former digital analyst at Cambridge Analytica leaked the company's illegitimate practices of extracting, using, and combining user data for targeting purposes. Then, microtargeting became a standard campaign practice—especially in the US—despite being debated controversially (e.g., Donald Trump's team invested 44 million dollars, and Hillary Clinton's team 28 million dollars in digital advertising during the 2016 presidential campaign; Frier, 2018). Digital political advertising and microtargeting can be observed in Europe as well: During the German federal election campaign in 2017 and the European election campaign in 2019, German political parties invested in digital advertising on Facebook and Google. In 2017, the Left (*Die Linken*) invested 450,000 euros, the Greens (*Die Grünen*) two million euros, and the Free Democratic Party (FDP) 500,000 euros (Scherfig, 2017). In 2019, German parties invested up to 558,001 euros in digital advertising, e.g., the Christian Democratic Union (CDU) spent 296,001 euros on Facebook ads and 261,200 euros

on digital advertising on Google (Hegelich & Medina Serrano, 2019). An analysis of microtargeting strategies showed that the Greens reached more women than men and that the Social Democratic Party (SPD) and FDP tended to reach people aged 25 to 44, indicating that the parties employed demographic targeting strategies (Hegelich & Medina Serrano, 2019). Hence, although political parties in the US invest more resources in terms of time and money in political microtargeting than political parties in Germany, and despite the fact that (a) the European Union's restrictive General Data Protection Regulation (GDPR) regulates data collection, storage, and usage in Germany (Zuiderveen Borgesius et al., 2018); and (b) an even more far-reaching code of conduct was recently co-developed by the digital industry and the European Commission (2019), political microtargeting is a hot topic in Germany that has evolved in parallel with technological developments in this field.

In fact, a large majority of the public is concerned: 62% of US citizens say that political targeting is not acceptable (Smith, 2018), while 89% of Germans demand more transparent labeling and regulation of political ads (MANRW, 2019), demonstrating the relevance of analyzing and clarifying targeting processes and their implications for users. In addition, voters view the violation of their privacy as problematic and are afraid of losing control over their personal data (MANRW, 2019), which can be a serious problem from a psychological perspective (see Section 5).

The goal of our work is to theoretically examine the relations between microtargeting and online privacy in the context of elections and social media affordances. We aim to contribute to current research on political microtargeting by providing an in-depth understanding of what social media users need and expect in terms of their individual online privacy. We elaborate on how online privacy behavior might evolve over time—from the initial assessment of one's goals when using social media, to exposure to political targeting, subsequent privacy considerations and behaviors—by analyzing previous research in the field of online privacy and political behavioral targeting and drawing upon the social media privacy model (Trepte, 2020; cf. Figure 1).

2. Political Targeting: The Relevance of a Psychological Perspective

Political microtargeting is a specific kind of campaign tool. As part of microtargeting, behavioral (e.g., website visits), sociodemographic (e.g., gender, age), network (e.g., communication partners), and meta data (e.g., time and place of a message) are collected, analyzed, and processed (Dobber et al., 2019; Papakyriakopoulos et al., 2017). This data is used to identify groups of similar users (Queck, 2018). These groups are then exposed to messages tailored to their assumed needs and preferences (Beer et al., 2019; Bol et al., 2020). This kind of collected *behavioral* data is often enriched and aggregated with *psychometric* data, making it possible to match adverts to users' personality, which can further increase persuasiveness and influence actual behavior (e.g., 50% more purchases of a product after matching the appearance of a product ad to users' personality; see Matz et al., 2017). Psychometric measures are either extracted from paralinguistic traits or provided by the users themselves. For example, users may actively fill out personality tests on Facebook (e.g., myPersonality App), with which companies connect different kinds and sources of data (see also Kosinski et al., 2013). Hence, behavioral political targeting is oftentimes combined with psychological targeting. In this article, we refer to both kinds of targeting as well as their combination as (political) microtargeting.

Microtargeting is deployed at the back-end by political parties who strive to inform, steer, and persuade potential voters. However, this is not noticeable to users at the front-end. Oftentimes, targeted information is perceived as conventional social media information or even as independent news. Only one third of social media users are aware that political targeting takes place (Dobber et al., 2018). However, even if users are aware of the practice of political targeting, they are not able to completely shield their posts and profiles from psychological or behavioral profiling. Thus, they may have to deal with the potentially uncomfortable sentiment of being objectified and assigned to a certain cluster.

By identifying target groups, it becomes possible to address users' concrete political attitudes, needs, and fears (Queck, 2018). For political parties, the advantages of microtargeting lie in the higher probability of addressing voters' specific expectations, in resource efficiency, and in staying competitive with other parties (König, 2020; Zuiderveen Borgesius et al., 2018). This approach was particularly evident during Barack Obama's 2008 election campaign, when the campaign team analyzed data sets from around 150 million people and divided them into interest groups that could be specifically targeted through various channels—such as email, social media advertisements, and home visits—although this example received little public attention at the time (Aaker & Chang, 2009). Then, after Donald Trump became US president in 2017, it was revealed that the British political consulting company Cambridge Analytica used Facebook users' data to create psychometric personality profiles for over 50 million individuals that were used for microtargeting purposes during Trump's campaign (Beuth & Horchert, 2018). In spring 2018, whistleblower and former Cambridge Analytica employee Christopher Wylie leaked background information on how Cambridge Analytica had set up an extensive system of websites and blogs to target voters with precisely tailored information (Baetz & Zilm, 2018).

Academics, lawyers, activists, and journalists (Bennett & Lyon, 2019; Potthast, 2019; Rebiger, 2018; Reihs, 2019) have criticized political microtargeting as intrusive and manipulative, because targeted users are often unaware of their exposure to this campaign

strategy. Despite restrictions regarding the processing of personal data in the EU (e.g., due to the GDPR), Twitter's official prohibition on political microtargeting (Fanta, 2018), and contextual limitations such as budget or party structures (Kruschinski & Haller, 2017), users provide a great deal of data on social media that can be used to target them *despite* these legal and contextual restrictions (Papakyriakopoulos et al., 2017). Subsequently, social network sites such as Facebook still present adverts and content to their users based on their *likes*, interests, and provided information, which is sometimes related to political topics (Facebook Help Center, 2021). At the same time, politicians increasingly use social media to directly address potential voters (Hegelich & Shahrezaye, 2015). Dobber et al. (2019, p. 7) summarize: "In sum, Europe's privacy laws do not categorically prohibit microtargeting. Still, Europe's privacy laws make microtargeting more difficult than in, for instance, the US."

While users' concerns are evident, the effects of political targeting are ambiguous. Research on the direct effect of political targeting on "outcome" variables such as voting behavior is scarce, and studies reveal a heterogeneous picture.

We suggest three main reasons for why it is difficult to find a linear relationship between exposure to political microtargeting and political participation outcomes. First, it is questionable whether the actions that facilitate microtargeting (e.g., tracking, tracing, or buying user data) provide information that is not already available through traditional sources like voter rolls and past voting behavior (Hersh, 2015). Second, potential effects of microtargeting on political outcomes can only be measured clearly if microtargeting presents unique information the user is not also exposed to through other channels. For example, if a social media user is targeted via both canvassing and microtargeting, the differential effect of microtargeting can only be measured if different information is conveyed through these two kinds of campaigning. Third, targeting is oftentimes applied coarsely. For example, German parties usually target based on broad categories such as gender and region (Hegelich & Medina Serrano, 2019). Such categories might not have strong effects on political participation.

The belief that targeting might have no direct effect on voters' decisions may be a source of relief—but should it be? We doubt this. Instead, we pose the overarching question of what exactly the "outcome" of targeting practices is. Therefore, it is important to significantly broaden our understanding of this "outcome." We seek to consider not only the narrow behavioral outcome, but also the question of whether and how political microtargeting affects social media users' and therefore voters' subjective self-perception of informational self-determination as well as perceived privacy and privacy concerns. Users' privacy perceptions may in turn also mediate their voting behavior. In other words, a lacking linear relationship between exposure to political microtargeting and political behavior could stem from a missing link to privacy mechanisms. Since identifying the psychological processes underlying how microtargeting is perceived with regard to privacy would require comprehensive theoretical and empirical investigations that go beyond the scope of a single journal article, we decided to begin working on this task theoretically. While previous theoretical work has analyzed political microtargeting and its potential consequences from a normative and communication science perspective (Haller & Kruschinski, 2020; König, 2020), a psychological perspective is still missing.

3. Users' Assessment of Privacy and Political Microtargeting

The concept of online privacy has been researched and defined in many distinct disciplines, such as communication science, psychology and sociology, applying descriptive, empirical, and normative perspectives (Masur, 2019; Schäwel, 2019; Sevignani, 2016; Trepte & Reinecke, 2011). Originally, privacy was normatively defined as the human "right to be let alone" (Warren & Brandeis, 1890, p. 193). The level of access an individual feels comfortable with and individual communication goals are crucial for privacy decisions (Dienlin, 2014; Trepte, 2020): In an "initial assessment" (cf. Figure 1, first row), users evaluate their individual level of access (e.g., high access through the disclosure of personal information like gender or political attitudes) and consider it in light of their individual communication goals (e.g., letting others know their personal information). The level of access to the self represents a pivotal component of personal privacy. Westin (1967, p. 7) defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Social media privacy is always defined in reference to certain others (e.g., institutions, people, or entities; Trepte, 2020). When writing a post to share on Twitter or Facebook, different people might assess the situation in different ways. One person might evaluate their privacy with regard to the service provider, while another person might consider not the provider but rather their followers. Hence, the service provider is an object of privacy assessments for the first person, but not the second. This level of access determines the decision an individual will make in a particular privacy-relevant situation. It is inter-individually different, has some intra-individual stability, and is context-dependent.

4. Social Media Boundary Conditions: Content and Affordances

Privacy regulation behavior is influenced by the social media context and its "boundary conditions" (cf. Figure 1, second row). Social networking sites such as Twitter or Facebook constitute important sources of political information. Social media as a context must therefore be

understood comprehensively in order to understand privacy, and in turn, the relevance of the mechanisms of control, trust, and communication (Nissenbaum, 2010). Hence, we will consider social media affordances that shape users' individual perceptions of privacy, control, trust, and communication options. The term affordance (Gibson, 2014) captures the idea that the environmental properties of an entity are perceived and experienced differently by different people. Here, the environmental properties would be social media affordances such as persistence, and the entity would be the social media site itself. While using social media, certain properties are actively used and emphasized, while others are overlooked (Trepte, 2015). Due to the importance of social media affordances for users' perceptions of online privacy, we will consider them in our theoretical investigation of the privacy-relevant context of political microtargeting.

We concentrate on the four affordances addressed in the social media privacy model (Trepte, 2020): anonymity, editability, association, and persistence (Evans et al., 2017; Treem & Leonardi, 2012). Other affordances discussed in the literature are visibility, navigability, interactivity (Evans et al., 2017), and paralinguistic affordances (Hayes et al., 2016).

In the social media context, "anonymity" means that other users, institutions, and companies do not know the source of a message (Evans et al., 2017), which can increase senders' perception of privacy. However, using social media anonymously is rare, because anonymity reduces contacts and social support, which are the main benefits of using social media (Rainie et al., 2013). Additionally, users leave data traces while searching the internet even when they appear anonymous to their online contacts. Companies specialized in collecting and aggregating data traces can create profiles that make it possible to identify the person and connect this data to their online personas. Therefore, anonymity with respect to companies and institutions is not guaranteed on social media (Trepte, 2020). Parties can use these data traces to optimize algorithms for microtargeting, for instance, by linking geospatial data with user interests (Dobber et al., 2019) or expressions of political views and opinions (e.g., through *likes*), which in turn allows them to better match the advertisements presented to users (Papakyriakopoulos et al., 2018). Furthermore, by joining a social media site and by accepting its terms and conditions, users (have to) consent to the further processing and use of their data for commercial or other purposes (Papakyriakopoulos et al., 2018) and thus implicitly—and often unawarely—also consent to political microtargeting. If users encounter tailored political advertisements and recognize that these are based on their private information, they might feel that their anonymity, and thus an essential part of their privacy, has been threatened. The question is, how would this impression affect the perception of potential privacy regulation mechanisms (see also Section 5)? Since political parties can acquire metadata that allows for targeted and personalized political advertisements from data broker companies; control cannot be used as a possible privacy mechanism without abandoning the use of the internet or a certain app (Dobber et al., 2018; Papakyriakopoulos et al., 2018). Legal norms, in turn, do not yet have a firm grip on targeting practices that are seen critically and even as illegitimate by activists and scientists. Therefore, legal norms offer only limited protection, meaning that the only available privacy mechanism is trust that one's data will be used responsibly. More interested and active voters might also consider communication with political parties as a privacy mechanism; however, there are no firm research results on whether social media users take advantage of this deliberative option. The mechanisms of control, trust, norms, and communication will be explained in more detail in Section 5.

"Editability" gives users the opportunity to adjust with whom they communicate in which manner (Treem & Leonardi, 2012) by modifying their posts or applying specific privacy settings (e.g., blocking people or designating the audience for specific posts). Users can also manage their self-presentation via social media functionalities that afford editability (e.g., editing a photo) and in this way regulate their privacy. For instance, a user might blur a photo or crop a picture in which she participates in a (political) demonstration to only show certain details. Messages or one's profile name can also be edited by means of functionalities that afford editability. Editing one's profile name can also be related to the anonymity affordance, such as when changing one's real name into a fake name.

A central affordance of social media is the "association" between different interaction partners (Ellison & boyd, 2013; Treem & Leonardi, 2012), which seldom allows a person to maintain control over the subjective regulation of privacy and therefore might reduce perceived privacy. The prevalence of the association affordance can influence users' number of contacts, quantity of interactions, network structures, the visibility of visited events and locations, group memberships, or pictures on Facebook. Fox and McEwan (2017) showed that associations between social media users negatively affect their sense of control. To counteract this, users can rely on alternative privacy mechanisms such as trust (see Section 5). Studies demonstrate that users with stronger associations trust their social media friends and acquaintances more (Hofstra et al., 2016). However, trust in Twitter and Facebook is comparatively low when it comes to political issues (Paus & Börsch-Supan, 2019). If a discrepancy between high trust in people and low trust in platforms or the source of a political advertisement is detected, the privacy mechanism of social and legal norms gains relevance. Users recall that social media platforms must adhere to social and legal norms ensuring that their personal data is used only in an acceptable, non-invasive way that follows data protection laws.

"Persistence" refers to the permanency and replicability of online statements and content (boyd, 2014). Data remains available over unknown periods of time and can be accessed by different and unexpected users, e.g., (future) employers (Evans et al., 2017; Treem & Leonardi, 2012) or political parties—although the GDPR requires "storage limitation" by stipulating that "personal data may not be retained for unreasonably long periods" (GDPR, 2018). Users do in fact see the lack of control over their personal information that results from the persistence of online information as a problem for their privacy (Teutsch et al., 2018).

According to the social media privacy model, the outlined affordances (i.e., social media boundary conditions) interact with users' ideal level of access to provide to their personal information and their communication goals (i.e., initial assessment), which in turn shape users' expectations about how they can react to potential privacy harms by using prevalent privacy mechanisms to regulate their privacy (cf. Figure 1, first to third row).

5. Available Privacy Mechanisms and the Experience of Privacy in the Context of Targeting

Control has long been and still is an essential part of the definition and understanding of privacy (Altman, 1974; Burgoon, 1982; Petronio, 2002). The basic assumption is that the amount of perceived privacy and corresponding informational self-determination depends on the control people perceive to have over their private information. Thus, more control equals more privacy. However, this linear relationship has not been supported by research so far (see Trepte, 2020). A decreasing amount of control does not necessarily mean having no or limited privacy. If a social media user trusts a provider like Twitter or a political party to handle their personal data responsibly, they rely on trust as a privacy mechanism, resulting in a perception of individual privacy. Changes in the person's privacy perceptions of Twitter's or the political party's trustworthiness will influence their privacy regulatory behavior. Hence, users are not restricted to one privacy mechanism, but can consider different mechanisms depending on their current availability and perceived impact. In the following paragraphs, we will describe each of the "available privacy mechanisms" (cf. Figure 1, third row) in detail.

Informational "control" means the ability to hold information back (Crowley, 2017) and the user's ability to freely choose whether to disclose certain information (e.g., political attitudes) or not (Tavani, 2007). In contrast to other privacy mechanisms such as communication, the individual him- or herself steers control behavior (i.e., "egocentric regulation," cf. Figure 1). Users can exercise control by anonymizing or editing their posts or profiles (e.g., by providing fake information). We assume that users who *feel* to be in control also *experience* more privacy than those who have no access to this mechanism. Users exercising control should therefore feel less susceptible to being targeted with personalized advertisements. However, control is hard to achieve and is only one aspect influencing the perception of privacy (Trepte, 2020). If users feel a lack of control, trust in the communication partner (e.g., a political party) becomes relevant. Trust in an online shop, for instance, is associated with a lower perception of risk regarding the disclosure of personal information (Gurung & Raja, 2016). Accordingly, if users have a strong feeling of trust towards a political party, they might feel a lower need for control in order to protect their privacy against this party's microtargeting practices. If, on the other hand, the user receives political advertising from a political party they highly mistrust, this could reduce their experience of privacy and increase the relevance of control or alternative privacy mechanisms.

"Interpersonal communication" is understood here as interactions between users, or between users on the one hand and institutions or companies on the other. For example, users might discuss among one another whether or not certain (political) opinions should be shared on Facebook. Furthermore, if the current privacy situation is not satisfactory, e.g., because users' social contacts might leak private information or no laws to protect privacy exist, users can engage in interpersonal communication with peers, companies or political parties to change the situation. In the case of political targeting, when privacy-invasive practices are recognized or gain public attention, such communication might take the form of problem-oriented interactions with peers or parties. We assume that users who anticipate that they can get in touch with the political party experience more privacy than users without access to such interpersonal communication. On the other hand, users sometimes feel powerless when communicating with companies about data deletion or terms of consent (Teutsch et al., 2018). Thus, interpersonal communication is not always possible or expedient for privacy regulation.

Instead, "trust" as the result of previous successful communication or adherence to norms can serve as a privacy regulatory mechanism. Trust is defined as the expression of balanced communication and the anticipation that normatively correct behavior will be implemented (Green, 2007). Trust and communication influence each other in the sense that a minimal level of trust is needed for communication, and trust can increase as a result of a successful communication (Saeri et al., 2014). Henderson et al. (2016) found that engaging in communication based on collectively established communication norms can predict trust in virtual teams. Common norms in online communities have a direct influence on users' trust in community members (Blanchard et al., 2011). Furthermore, trust can even reduce privacy concerns (Taddei & Contena, 2013), suggesting that people might be less concerned about a political party or social media site they trust. However, Lankton et al. (2012) demonstrated that trust cannot be a full substitute for control. A study on political microtargeting conducted

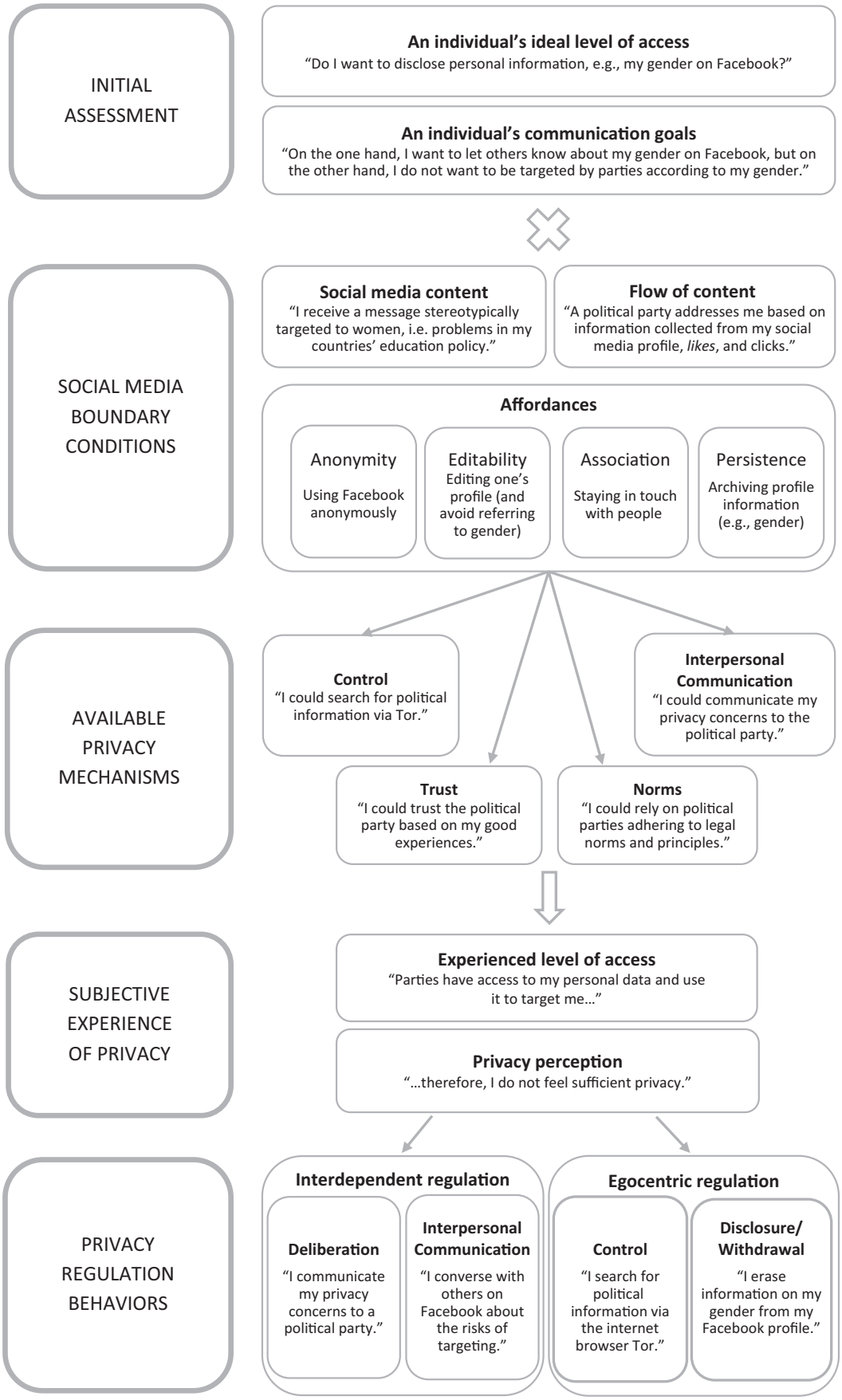

Figure 1. The social media privacy process as experienced by users confronted with political behavioral targeting: From the initial assessment of individual needs to the behaviors and choices ultimately executed to regulate one's privacy. Source: Trepte (2020).

in the Netherlands found that a political party post that was clearly marked as an advertisement had no effect on trust in this party. Still, users were less willing to share this post that they knew was advertising by a political party (Kruikemeier et al., 2016). The study's authors conclude that users resist sharing political messages that they know to be personalized political ads (Kruikemeier et al., 2016).

Next, social and legal "norms" play an important role in privacy regulation. If social media users have the feeling that the existing norms in place protect them sufficiently, their experience of privacy should be correspondingly high. Social norms can evolve either as a result of observations, i.e., what do I *see* others doing (Lewis, 2011), or as a result of assumptions, i.e., what do I *believe* others are doing regarding their privacy (Spottswood & Hancock, 2017) or protecting others' privacy (e.g., third parties follow the law in order to protect users' privacy). While the influence of social norms on social media users' privacy has already been investigated (Utz & Krämer, 2009), there has been no research into how legal norms and regulations influence privacy behaviors in the context of political microtargeting. The perception and awareness of legal norms may be associated with and affected by current law, which demands "lawfulness, fairness, and transparency," "purpose limitation," "data minimization," "accuracy," "storage limitation," "integrity and confidentiality," and "accountability" when processing personal data (GDPR, 2018). Thus, users may rely on third parties adhering to these principles and consequently following not only the law but also legal norms of transparency and fairness. In such a case, they should experience more privacy. This is also related to the trust mechanism. Users who trust political parties probably trust them to follow these principles as well.

This process of users' initially assessing (communication) goals, perceiving social media affordances and available privacy mechanisms, and arriving at a subjective experience of privacy and subsequent privacy behavior (which is explained in more detail in Section 6) is visualized in the social media privacy model (Trepte, 2020), which we enriched with concrete examples regarding political targeting.

6. Users' Privacy Regulation in the Face of Targeting

According to the social media privacy model (Trepte, 2020), the individual perception of privacy can vary depending on available privacy mechanisms and in turn lead to different regulatory behaviors, namely interdependent (deliberation/interpersonal communication) or individual (control/disclosure or withdrawal) regulation. This means, for example, that if the privacy mechanism control is available and the experienced level of privacy is low, no deliberative communication is performed. Instead, control would be exercised as a regulating behavior (e.g., using the Tor internet browser to search for political information; cf. Figure 1, last row). However, when the control mechanism is not available, the availability of alternative mechanisms becomes relevant, which in turn affects users' perceived privacy and regulatory behaviors. Consequently, either interdependent (e.g., negotiating with third parties or communicating with users) or individual (e.g., limiting personal disclosures) regulatory strategies are enacted (cf. Figure 1, last row). Regulation of behavior should be increasingly implemented the lower the perception of privacy is (e.g., by rejecting specific cookies or services). However, a current survey conducted in Germany revealed that 20% of 1,065 participants did not use any settings to actively protect their privacy (i.e., privacy regulation) during the past year, although 82% expressed concerns about their privacy (Kozyreva et al., 2020).

Still, users might have a limited perception of political targeting because it is designed to not be perceived by users. Hence, privacy behaviors are not a direct reaction to exposure to political targeting, but presumably a reaction to some general (perhaps limited) knowledge of political targeting practices, associated attitudes, and expectations about which privacy mechanisms might successfully combat these kinds of practices. We will now refer to how future research and debates may address this particular circumstance.

7. Discussion

Privacy is a higher-order need and as such oftentimes remains in the background while predominantly serving the fulfilment of other needs, such as participation in democratic processes (Trepte & Masur, 2017). The need for privacy particularly comes into play and causes friction when it is unfulfilled. This is the case when it comes to political targeting. Based on the social media privacy model, we propose considering users' assessment of access and communication goals; social media boundary conditions, including prevalent affordances; available privacy mechanisms; subjective experiences of privacy; and potential interdependent or egocentric privacy regulation behaviors in the context of microtargeting processes. As such, individual privacy regulation becomes visible and is not modeled simply as disclosure or withdrawal, but also as a form of political action. Accordingly, there are interdependent regulation strategies like interpersonal communication and deliberation, in which the individual communicates conscious decisions about privacy and levels of access.

Our theoretical analysis showed that the effects of political microtargeting are determined by users' need for privacy and their assessment of the social media context in light of this need. As an analytical result of our theoretical discussion, we present three propositions for future research.

Our first proposition is to further consider the complexity of the social media context, users' perception of it, and its affordances. It is important to understand what kinds of targeting users are exposed to via which

channels (i.e., context). Then, not only exposure, but also users' perception of the context and information processing must be measured (i.e., perceptions). Finally, the perceived social media functionalities and boundaries must be evaluated (i.e., affordances). Exposure to political targeting does not necessarily mean that users are aware of it. Indeed, only one-third of users are even aware that targeting takes place (Dobber et al., 2018). Thus, only when we know what users experience can we understand how this affects privacy and informational self-determination, as well as ultimately the dependent outcome variable. This consideration has a crucial impact on methodology, which will be discussed in the third proposition (see also Bol et al., 2020).

Our second proposition is to bring privacy to the fore and to understand users' privacy perception and evaluation as underlying psychological processes that influence or even mediate the consequences of microtargeting (i.e., the outcome). Our theoretical analysis showed that the level of individual privacy is a core aspect of self-determination and a precondition for valuable online experiences, which in turn affect numerous decisions, actions, and behaviors. This is of interest with regard to the effectiveness and potential intrusiveness of political microtargeting strategies—from both political parties' as well as researchers' point of view.

Our third proposition is to conduct research that aligns with the ethical principles formulated for social science. Our theoretical analysis showed that users feel uncomfortable being observed, evaluated, and targeted. Another ethical concern is that most users are not aware *that* targeting takes place (Dobber et al., 2018). Even if they are aware of it, they cannot influence *what* data is being seen and used, and *when and how* this data is reflected back to them in the form of targeted advertising (Matz et al., 2017, 2020; Noecker et al., 2013).

This ethical criticism is closely connected to empirical possibilities and research practices in the field of political behavioral targeting (e.g., tracking or tracing user data). In future research on targeting and privacy, it will be important to rely on observational studies and computational approaches to gather useful data, for which ethical boundaries will pose one of the most serious challenges. One reason why observational measures are needed is because users' self-reports are often not reliable in the context of political microtargeting: Users have difficulties identifying situations in which they were targeted and how they felt. Therefore, more advanced observational and experimental research designs are needed (Bol et al., 2020). In tracking studies, for instance, participants would install a browser plug-in on their computer or smartphone to log their online behavior and allowing to draw conclusions based on their clicks (which might in turn have been guided by specific ads). However, this method does also not allow for investigating users' experience of privacy. Thus, even more comprehensive and intelligent measures are required, e.g., combining users' log data and self-reports to identify the moment and source of targeting and initiate a direct request for a user self-report. The crucial point with such tracking or tracing methods is that they are based on similar mechanisms as microtargeting (i.e., observing users and specifically targeting them based on these observations). Consequently, user-centered research on the effects of political microtargeting presumes certain ethical standards that should also hold in the field of targeting resarch itself.

8. Conclusion

The goal of this theoretical investigation of privacy and political microtargeting on social media was to derive propositions for analyzing political microtargeting in a way that considers users' privacy needs, relevant political outcomes, and ethical implications. We conclude by highlighting the importance of: (a) considering the complexity of the social media context and its affordances as well as users' perceptions of these, (b) positioning privacy as a relevant research topic by understanding how users' privacy experiences influence and mediate the outcome of microtargeting, and (c) conducting research in accordance with ethical guidelines in order to establish research practices that meet the standards we as scholars set for the social media industry.

Acknowledgments

We would like to thank Jennifer Müller for her support and valuable feedback.

Conflict of Interests

The authors declare no conflict of interests.

References

Aaker, J., & Chang, V. (2009). Obama and the power of social media and technology. *The European Business Review*, 16–32. https://jaaker.people.stanford.edu/sites/g/files/sbiybj2966/f/obamaandthepowerofsocialmediafinal2009.pdf

Altman, I. (1974). Privacy: A conceptual analysis. In S. T. Margulis (Ed.), *Man-environment interactions: Evaluations and applications* (pp. 3–28). Dowden, Hutchinson & Ross.

Baetz, B., & Zilm, K. (2018, April 10). *Daten ohne Schutz—Zuckerberg in Bedrängnis* [Data without protection—Zuckerberg in trouble]. Deutschlandfunk. https://www.deutschlandfunk.de/der-facebook-skandal-daten-ohne-schutz-zuckerberg-in.724.de.html?dram:article_id=415251

Beer, D., Redden, J., Williamson, B., & Yuill, S. (2019). *Landscape summary: Online targeting: What is online targeting, what impact does it have, and how can we maximise benefits and minimise harms?* Centre for Data Ethics and Innovation. http://orca.cf.ac.uk/126114

Bennett, C. J., & Lyon, D. (2019). Data-driven elections: Implications and challenges for democratic societies. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1433

Beuth, P., & Horchert, J. (2018, March 20). Was treibt eigentlich Cambridge Analytica? [What is Cambridge Analytica doing?]. *Spiegel*. https://www.spiegel.de/netzwelt/netzpolitik/cambridge-analytica-das-steckt-hinter-der-datenanalyse-firma-a-1198962.html

Blanchard, A. L., Welbourne, J. L., & Boughton, M. D. (2011). A model of online trust. *Information, Communication & Society*, *14*(1), 76–106. https://doi.org/10.1080/13691181003739633

Bol, N., Strycharz, J., Helberger, N., van de Velde, B., & de Vreese, C. H. (2020). Vulnerability in a tracked society: Combining tracking and survey data to understand who gets targeted with what content. *New Media & Society*, *22*(11), 1996–2017. https://doi.org/10.1177/1461444820924631

boyd, d. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Burgoon, J. K. (1982). Privacy and communication. *Communication Yearbook*, *6*(1), 206–249. https://doi.org/10.1080/23808985.1982.11678499

Crowley, J. L. (2017). A framework of relational information control: A review and extension of information control research in interpersonal contexts. *Communication Theory*, *27*(2), 202–222. https://doi.org/10.1111/comt.12115

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* [Media and privacy] (pp. 105–122). Karl Stutz.

Dobber, T., Ó Fathaigh, R., & Zuiderveen Borgesius, F. J. (2019). The regulation of online political microtargeting in Europe. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1440

Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. H. (2018). 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

Ellison, N. B., & boyd, d. (2013). Sociality through social network sites. In W. H. Dutton (Ed.), *The Oxford handbook of internet studies* (pp. 151–172). Oxford University Press.

European Commission. (2019). *Guidelines on ethical standards for the participation of the members of the european commission in the election campaign*. https://ec.europa.eu/info/sites/info/files/guidelines_election_campaign_en.pdf

Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2017). Explicating affordances: A conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication*, *22*(1), 35–52. https://doi.org/10.1111/jcc4.12180

Facebook Help Center. (2021). *How does Facebook decide which ads to show me?* Facebook. https://www.facebook.com/help/516147308587266/how-ads-work-on-facebook/?helpref=hc_fnav

Fanta, A. (2018). *EU-kommission: 80 Prozent der Europäer wollen wissen, wer für politische Werbung im Netz zahlt* [EU Commission: 80 percent of Europeans want to know who pays for political advertising on the web]. Netzpolitik. https://netzpolitik.org/2018/eu-kommission-80-prozent-der-europaeer-wollen-wissen-wer-fuer-politische-werbung-im-netz-zahlt

Fox, J., & McEwan, B. (2017). Distinguishing technologies for social interaction: The perceived social affordances of communication channels scale. *Communication Monographs*, *84*(3), 298–318. https://doi.org/10.1080/03637751.2017.1332418

Frier, S. (2018, April 3). Trump's campaign said it was better at Facebook. Facebook agrees. *Bloomberg*. https://www.bloomberg.com/news/articles/2018-04-03/trump-s-campaign-said-it-was-better-at-facebook-facebook-agrees

General Data Protection Regulation. (2018). *Art. 5: Principles relating to processing of personal data*. https://gdpr-info.eu/art-5-gdpr

Gibson, J. J. (2014). *The ecological approach to visual perception*. Routledge.

Green, M. C. (2007). Trust and social interaction on the internet. In A. N. Joinson, K. Y. A. McKenna, T. Postmes, & U. D. Reips (Eds.), *The Oxford handbook of Internet psychology* (pp. 43–52). Oxford University Press.

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security*, *24*(4), 348–371. https://doi.org/10.1108/ICS-05-2015-0020

Haller, A., & Kruschinski, S. (2020). Politisches Microtargeting: Eine normative Analyse von datenbasierten Strategien gezielter Wähler_innenansprache [Political microtargeting: A normative analysis of data-based strategies of targeted voters]. *ComSoc Communicatio Socialis*, *53*(4), 519–530. https://doi.org/10.5771/0010-3497-2020-4-519

Hayes, R. A., Carr, C. T., & Wohn, D. Y. (2016). One click, many meanings: Interpreting paralinguistic digital affordances in social media. *Journal of Broadcasting & Electronic Media*, *60*(1), 171–187. https://doi.org/10.1080/08838151.2015.1127248

Hegelich, S., & Medina Serrano, J. C. (2019). *Microtargeting in Deutschland bei der Europawahl 2019* [Microtargeting in Germany in the 2019 European elections]. Media Authority of North Rhine-Westphalia. https://www.blm.de/files/pdf2/studie_microtargeting_deutschlandeuropawahl2019_hegelich-1.pdf

Hegelich, S., & Shahrezaye, M. (2015). The communication behavior of German MPs on Twitter: Preaching to the converted and attacking opponents. *Euro-*

pean Policy Analysis, *1*(2), 155–174. https://doi.org/10.18278/epa.1.2.8

Henderson, L. S., Stackman, R. W., & Lindekilde, R. (2016). The centrality of communication norm alignment, role clarity, and trust in global project teams. *International Journal of Project Management*, *34*(8), 1717–1730. https://doi.org/10.1016/j.ijproman.2016.09.012

Hersh, E. D. (2015). *Hacking the electorate: How campaigns perceive voters*. Cambridge University Press. https://doi.org/10.1017/CBO9781316212783

Hofstra, B., Corten, R., & van Tubergen, F. (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior*, *60*, 611–621. https://doi.org/10.1016/j.chb.2016.02.091

König, P. D. (2020). Why digital-era political marketing is not the death knell for democracy: On the importance of placing political microtargeting in the context of party competition. *Statistics, Politics and Policy*, *11*(1), 87–110. https://doi.org/10.1515/spp.2019--0006

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Scienses*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Kozyreva, A., Herzog, S., Lorenz-Spreen, P., Hertwig, R., & Lewandowsky, S. (2020). *Artificial intelligence in the online environment: A representative survey on public opinion in Germany*. Max Planck Institute for Human Development. https://www.conpolicy.de/en/news-detail/artificial-intelligence-in-the-online-environment-a-representative-survey-on-public-opinion-in-germ

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

Kruschinski, S., & Haller, A. (2017). Restrictions on data-driven political micro-targeting in Germany. *Internet Policy Review*, *6*(4). https://doi.org/10.14763/2017.4.780

Lankton, N. K., McKnight, D. H., & Thatcher, J. B. (2012). The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: An empirical test of intention to continue using a social networking website. *IEEE Transactions on Engineering Management*, *59*(4), 654–665. https://doi.org/10.1109/TEM.2011.2179048

Lewis, K. (2011). The co-evolution of social network ties and online privacy behavior. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 91–110). Springer.

Masur, P. K. (2019). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

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

Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the United States of America*, *114*(48), 12714–12719. https://doi.org/10.1073/pnas.1710966114

Media Authority of North Rhine-Westphalia. (2019). *Informationsverhalten bei Wahlen und politische Desinformation* [Information behavior in elections and political disinformation]. https://www.medienanstalt-nrw.de/fileadmin/user_upload/lfm-nrw/Service/Pressemitteilungen/Dokumente/2019/Praesentation_forsa_Desinformation_LFMNRW.pdf

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Noecker, J., Ryan, M., & Juola, P. (2013). Psychological profiling through textual analysis. *Literary and Linguistic Computing*, *28*(3), 382–387. https://doi.org/10.1093/llc/fqs070

Papakyriakopoulos, O., Hegelich, S., Shahrezaye, M., & Medina Serrano, J. C. (2018). Social media and microtargeting: Political data processing and the consequences for Germany. *Big Data & Society*, *5*(2). https://doi.org/10.1177/2053951718811844

Papakyriakopoulos, O., Shahrezaye, M., Thieltges, A., Medina Serrano, J. C., & Hegelich, S. (2017). Social Media und Microtargeting in Deutschland [Social media and microtargeting in Germany]. *Informatik-Spektrum*, *40*(4), 327–335. https://doi.org/10.1007/s00287-017-1051-4

Paus, I., & Börsch-Supan, J. (2019). *Alles auf dem Schirm?* [Everything in mind?]. Vodafone. https://www.vodafone-stiftung.de/alles-auf-dem-schirm

Petronio, S. (2002). *Boundaries of privacy*. State University of New York Press.

Potthast, K. C. (2019). *Political Microtargeting—Zwischen Regulierungsbegehren und Ungewissheit* [Political microtargeting—Between regulatory desire and uncertainty]. Juwiss. https://www.juwiss.de/103-2019

Queck, S. (2018). *Microtargeting—Definition, Einsatz und Beispiele* [Microtargeting—Definition, use and examples]. Marconomy. https://www.marconomy.de/microtargeting-definition-einsatz-und-beispiele-a-739666

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, privacy, and security online*. Pew Research Center. http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online

Rebiger, S. (2018). *Offener brief: Europäische Parteien sollen auf Microtargeting verzichten* [Open letter: European parties should renounce microtargeting]. Netzpolitik. https://netzpolitik.org/2018/offener-

brief-eu-parteien-sollen-auf-microtargeting-verzichten

Reihs, V. (2019). *Politisches Microtargeting in Deutschland: Ich sehe was, was du nicht siehst* [Political microtargeting in Germany: I see something you don't]. Politik-Digital. https://politik-digital.de/news/politisches-microtargeting-in-deutschland-ich-sehe-was-was-du-nicht-siehst-155876

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology*, *154*(4), 352–369. https://doi.org/10.1080/00224545.2014.914881

Schäwel, J. (2019). *How to raise users' awareness of online privacy* [Doctoral dissertation, University Duisburg-Essen]. DuEPublico2. https://doi.org/10.17185/duepublico/70691

Scherfig, L. (2017, January 26). *Wie die Parteien 2017 in den digitalen Wahlkampf ziehen* [How the parties are moving into the digital election campaign in 2017]. Berliner Morgenpost. https://www.morgenpost.de/politik/article209403515/Wie-die-Parteien-2017-in-den-digitalen-Wahlkampf-ziehen.html

Sevignani, S. (2016). *Privacy and capitalism in the age of social media*. Routledge.

Smith, A. (2018). *Algorithms in action: The content people see on social media*. Pew Research Center. https://www.pewresearch.org/internet/2018/11/16/algorithms-in-action-the-content-people-see-on-social-media

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication*, *22*(2), 26. https://doi.org/10.1111/jcc4.12182

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x

Teutsch, D., Masur, P. K., & Trepte, S. (2018). Privacy in mediated and nonmediated interpersonal communication: How subjective concepts and situational perceptions influence behaviors. *Social Media + Society*, *4*(2), 1–14. https://doi.org/10.1177/2056305118767134

Treem, J. W., & Leonardi, P. M. (2012). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. *Communication Yearbook*, *36*(1), 143–189. https://doi.org/10.1080/23808985.2013.11679130

Trepte, S. (2015). Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. *Social Media and Society*, *1*(1), 1–2. https://doi.org/10.1177/2056305115578681

Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, *19*(4), 1–22. https://doi.org/10.1093/ct/qtz035

Trepte, S., & Masur, P. K. (2017). Need for privacy. In V. Zeigler-Hill & T. K. Shakelford (Eds.), *Encyclopedia of personality and individual differences*. Springer. https://doi.org/10.1007/978-3-319-28099-8_540-1

Trepte, S., & Reinecke, L. (Eds.). (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer.

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Journal of Psychosocial Research on Cyberspace*, *3*(2), Article 2. http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

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

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, *14*(1), 82. https://doi.org/10.18352/ulr.420

About the Authors

Johanna Schäwel (PhD) is a postdoctoral researcher at the Institute of Communication Science: Media Psychology at the University of Hohenheim (Germany). Her research focuses on causes and consequences of social media use, especially users' (privacy) needs and competencies.

Regine Frener (MA, University of Mannheim) is a PhD candidate at the Institute of Communication Science: Media Psychology at the University of Hohenheim (Germany). She is interested in gender studies and how it relates to privacy and self-disclosure.

Sabine Trepte is a professor for media psychology at the University of Hohenheim (Germany). Her research focuses online self-disclosure and privacy from a psychological perspective.