JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 5, NO. 1, 2023, 23–47

COPING WITH ALGORITHMIC RISKS: HOW INTERNET USERS IMPLEMENT SELF-HELP STRATEGIES TO REDUCE RISKS RELATED TO ALGORITHMIC SELECTION

Kiran Kappeler[a], Noemi Festic[a], Michael Latzer[a] and Tanja Rüedy[a]

ABSTRACT

Algorithmic selection is omnipresent in various domains of our online everyday lives: it ranks our search results, curates our social media news feeds, or recommends videos to watch and music to listen to. This widespread application of algorithmic selection on the internet can be associated with risks like feeling surveilled (S), feeling exposed to distorted information (D), or feeling like one is using the internet too excessively (O). One way in which internet users can cope with such algorithmic risks is by applying self-help strategies such as adjusting their privacy settings (S_{strat}), double-checking information (D_{strat}), or deliberately ignoring automated recommendations (O_{strat}). This article determines the association of the theoretically derived factors risk awareness (1), personal risk affectedness (2), and algorithm skills (3) with these self-help strategies. The findings from structural equation modelling on survey data representative for the Swiss online population (N_{2018}=1,202) show that personal affectedness by algorithmic risks, awareness of algorithmic risks and algorithm skills are associated with the use of self-help strategies. These results indicate that besides implementing statutory regulation, policy makers have the option to encourage internet users' self-help by increasing their awareness of algorithmic risks, clarifying how such risks affect them personally, and promoting their algorithm skills.

Keywords: algorithmic risks; coping; self-help strategies; governance of algorithms; governance choice; survey method

[a] University of Zurich, Switzerland.

1 INTRODUCTION

An increasing share of our daily lives is spent online with endless options offered for a broad range of our needs, such as entertainment, information seeking, or socializing. To catch and maintain internet users' attention, online services (e.g., search engines, social media, streaming platforms) draw on algorithms to select the content with the highest probability of matching their users' interests. This algorithmic selection increasingly governs our daily lives, for instance, by ranking search results or news articles, recommending a certain movie, or curating one's social media feed (Festic, 2020; Latzer et al., 2016; Latzer & Festic, 2019). Hence, algorithms embedded in widespread online services affect our daily lives in many ways by automatically selecting pieces of information and assigning relevance to them (Latzer & Just, 2020). An input-throughput-output model helps to better grasp this understanding of algorithmic selection (Latzer et al., 2016): based on *input* data (e.g., users' click behavior, user requests), computational procedures (*throughput*) produce an algorithmically selected *output* (e.g., tailored news feeds, personalized recommendations).

While the widespread application of algorithms on the internet brings benefits like the reduction of complexity, it also entails challenges and risks for individuals and society as a whole (Just & Latzer, 2017; Latzer et al., 2016). Algorithmic selection relies on user data that is constantly being collected (Büchi et al., 2020; Hildebrandt, 2008). In many instances, internet users are not consciously sharing their data and are thus not aware of the data traces they produce (Micheli et al., 2018). The algorithmic processing of this collected data entails risks.

So far, research on algorithmic risks and how internet users cope with them predominantly focused on privacy (e.g., Boerman et al., 2018; Büchi et al., 2017). As a consequence of the increased collection of data and the widespread prevalence of algorithmic-selection applications (Ruckenstein & Granroth, 2020), further risks have been addressed. Key examples include worries about online *surveillance* based on the widespread tailoring of online contents (Ruckenstein & Granroth, 2020; Véliz, 2020; Zuboff, 2019), fears about *distorted information* through the algorithmic ranking of search results and news articles (Bozdag, 2013; Flaxman et al., 2016), and perceived *internet overuse* fostered by curated entertainment content by recommender systems (Gui & Büchi, 2019; Syvertsen, 2020). While concerns about the social risks of surveillance, distorted information, and internet overuse have existed before the spread of algorithmic-selection applications on the internet, the ubiquity of algorithms online renders their prevalence more severe; algorithmic selection significantly facilitates the unspecific collection and analysis of large amounts of personal data, the tailoring of contents based thereon as well as the allocation of personalized recommendations (Büchi et al., 2020).

Currently, statutory regulation (e.g., the General Data Protection Regulation (GDPR) in the European Union (EU)) as a governance mode to reduce such risks is increasing (see Larus et al., 2018). Despite this, a sense of helplessness and a wish for more control over opaque algorithms remain prevalent sentiments among internet users (Festic, 2020). Self-help strategies—such as adjusting one's privacy settings—provide a complementary governance choice for internet users to cope with algorithmic risks (Boerman et al., 2018; Latzer & Just, 2020). Therefore, how users engage with algorithmic-selection applications and cope with their risks warrants attention (Kitchin, 2017; Ramizo, 2021).

This article provides previously lacking nationally representative data on how internet users cope with algorithmic risks. By doing so, this study contributes to a better understanding of factors that are associated with internet users' self-help strategies when coping with diverse algorithmic risks. Our theoretical basis for these mechanisms lies in three approaches that seek to explain how people react to risks and try to reduce them, i.e., the protection motivation theory (Rogers, 1975), the health belief model (Rosenstock, 1974), and the integrated behavior model (Montaño & Kasprzyk, 2008). Derived from these theories we propose that the awareness of a risk, the affectedness by this risk, and the skills related to the risk are associated with the use of self-help strategies against it. In line with this, this article seeks to show how these three factors are associated with internet users' self-help strategies against three types of algorithmic risks: *How are the awareness of algorithmic risks (1), the personal affectedness by these risks (2), and algorithm skills (3) associated with internet users' self-help to cope with the three algorithmic risks surveillance (S), distorted information (D), and internet overuse (O)?*

To investigate this question, we use structural equation modelling (SEM) on survey data representative for the Swiss online population to determine the association of three theory-derived factors with internet users' self-help strategies to cope with algorithmic risks. Our findings contribute to the discussion about how internet users' self-help strategies can be promoted as an alternate governance mode in an otherwise difficult to regulate space.

2 THEORETICAL BACKGROUND AND EXTANT RESEARCH ON ALGORITHMIC RISKS AND COPING STRATEGIES

2.1 Algorithmic Risks

Algorithmic selection relies on the constant and automated collection of massive amounts of data (Büchi et al., 2020; Hildebrandt, 2008), which entails a range of diverse risks, like feeling surveilled (Ruckenstein & Granroth, 2020; Zuboff, 2019), having one's privacy violated (Véliz, 2020), seeing filtered and personalized content on search engines and social media (Swart, 2021) that can be biased (Bozdag, 2013), distorted (Flaxman et al., 2016), and manipulative (Petre et al., 2019), and feeling like one is spending more time online than intended (Gui & Büchi, 2019; Syvertsen, 2020), which can affect internet users' well-being (Büchi et al., 2019).

Whenever internet users do something online, their behavior leaves data traces (Micheli et al., 2018; Ruckenstein & Granroth, 2020). On one hand, internet users can actively generate data by producing content, for instance by uploading an image to a social networking site. On the other hand, internet users can also (unconsciously) generate data when browsing the internet, for example when googling a certain product or clicking on an advertisement. These data traces can be collected, tracked, mined and evaluated algorithmically (Micheli et al., 2018), which leads to an increased risk of *surveillance*, for instance by platforms, governments, organizations or peers (Büchi et al., 2020; Demertzis et al., 2021; Zuboff, 2019). Furthermore, algorithmically selected content differs between individual internet users as it can be adapted according to their past behavior and interests (Bozdag, 2013; Gillespie, 2014; Swart, 2021). This personalization can lead to an increase in *distorted information*. In addition, the internet's relevance for various aspects of our everyday life together with receiving automated recommendations can lead to an increase in time spent online. Consequently, internet users can feel like they spend too much time online, which translates into *perceived internet overuse* (Büchi et al., 2019; Syvertsen, 2020). While previous research into algorithmic risks and the ways in which internet users cope with them have focused primarily on privacy protection (e.g., Boerman et al., 2018), we seek to extend this research by focusing on these three: surveillance, distorted information, and perceived internet overuse. One aspect that these risks have in common is that internet users can actively cope with them by engaging in dedicated self-help strategies. These self-help strategies are introduced in the following section.

2.2 Regulation of Algorithmic Risks: Self-Help Strategies

Reducing the algorithmically fueled risks introduced above is a goal of risk-based regulatory approaches (Latzer & Just, 2020). Such governance modes include statutory regulation (e.g., the GDPR in the EU), market solutions, and self-regulation of the industry (Latzer, Saurwein, et al., 2019; Latzer & Just, 2020; Saurwein et al., 2015; Seyfert, 2021). Despite statutory regulation aiming at increasing users' sovereignty over their own data, many internet users wish for more control over algorithms (Festic, 2020). One governance mode (Latzer & Festic, 2019; Latzer & Just, 2020), which complements statutory regulation and industry self-regulation, is self-management by users, for instance of their privacy (Boerman et al., 2018). We argue that applying such *self-help strategies* is a valid complementary governance choice for internet users to cope with risks that are related to algorithmic selection. The term 'self-help' originates in the domain of psychology. It designates the adaptation of one's own behavior to cope with problems and has spilled into other academic fields as well as popular culture (see Illouz, 2008 for a critical appraisal of the term). Therefore, we use this term to highlight individuals exerting agency when coping with algorithmic risks.

From a user perspective, there are many ways to deal with algorithmic risks. To mitigate the *risk of surveillance*, internet users can try to make their online habits less traceable (Büchi et al., 2017; Micheli et al., 2018; Sánchez & Viejo, 2018), for instance, by adjusting their privacy settings, using virtual private networks (VPNs) (Longworth, 2018; Weinberger et al., 2017), using their browser's private mode, deleting cookies (Boerman et al., 2018; Park, 2015), or applying privacy-enhancing technologies like the browser add-on Ghostery (Ireland, 2020; Latzer & Just, 2020). Moreover, internet users can use online content selectively or even refrain from using certain services (Boerman et al., 2018) and thereby, produce less data that can be used as input for algorithmic selection. Such strategies can be understood as preventive (Ebbers, 2020). To alleviate the *risk of distorted information*, users can double check information that they see online, for instance displayed on their social media news feeds (Islam et al., 2020; Leeder, 2019). Thereby, they can react to the content that has been algorithmically curated for them in a critical way (Zarouali et al., 2017). Such behaviors can be seen as defensive (Ebbers, 2020). To reduce the *risk of perceived internet overuse*, internet users can limit their screen-time or abstain from using certain services (at certain times) (Syvertsen, 2020), or ignore the automated recommendations that they are shown online. They can also try to influence the algorithmic content they see, for instance, by (not) liking or (not) clicking on certain content to inform the algorithm about their interests and preferences (Cotter, 2019; Gan, 2017; Lowe-Calverley & Grieve, 2018; Marder, 2018) or by (un-)following accounts or hiding certain posts in their timeline (Swart, 2021).

In sum, internet users can apply a variety of self-help strategies when interacting with algorithmic-selection applications to cope with the risks their use can entail. The degree to which self-help strategies pose an effective way to mitigate algorithmic risks remains difficult to estimate due to the black-box nature of algorithmic selection and the opacity of the services in which it is embedded (Kitchin, 2017). Still, taking action by applying such self-help strategies is a way in which internet users exert agency and regain autonomy in the digital space. As has been shown for privacy protection behavior (Büchi et al., 2021), the application of protective behavior is highly unequally distributed in digital societies. To understand who applies self-help strategies online to cope with algorithmic risks, the following section introduces a set of important factors to consider in this context.

2.3 Factors Associated with the Use of Self-Help Strategies

The theoretical approaches that build the basis for our model explaining how different factors influence how internet users cope with algorithmic risks originate in the realm of health protective behavior. These models were originally conceptualized to explain with what factors behaviors against health risks (e.g., smoking cessation, HIV-prevention) are associated. Recently, such approaches have been transferred to the field of communication research to study protective behavior that reduces risks that internet use entails, like risks related to privacy protection or online behavioral advertising (e.g., Boerman et al., 2018; Ham, 2017). The use of these approaches brings the benefit of applying established theories on behavioral mechanisms to a new context. This article's hypotheses are rooted in three such theoretical approaches: the protection motivation theory (Rogers, 1975), the health belief model (Rosenstock, 1974), and the integrated behavior model (Montaño & Kasprzyk, 2008). Taken together, these approaches propose that whether and to what extent a person applies certain behaviors to reduce a specific type of risk depends on the perceived severity of this risk and the perceived personal susceptibility to it, as well as on a person's knowledge about and attitude towards it. We transfer these theoretical approaches that are geared towards explaining protective behavior against risks in more general terms to the field of algorithmic risks. Hence, we integrate these three theoretical approaches to explain what factors are associated with internet users' self-help strategies against algorithmic risks. For each of these factors, we will show how these theoretical approaches together with existing research led to our hypotheses.

2.3.1 Risk Awareness and Self-Help Strategies

To begin with, the protection motivation theory (Rogers, 1975) and the health belief model (Rosenstock, 1974) propose that the perceived severity of a risk influences whether someone intends to apply protective behaviors to reduce a risk. Findings about the relationship between concerns and protection strategies in the field of online risks differ according to type of protection measures that are applied. For instance, no or only a partial relation between privacy-related concerns and the (non-)use of social networking sites (Baruh et al., 2017) or smart speakers (Lutz & Newlands, 2021) has been found. At the same time, an association between privacy concerns and the general use of protection measures has been found by several survey studies (e.g., H. Chen et al., 2017; Dienlin & Metzger, 2016 for SNS; Ireland, 2020), including a meta-analysis of studies on privacy management (Baruh et al., 2017). A two-wave panel study (Boerman et al., 2018) that applied the protection motivation theory (Rogers, 1975) to privacy protection online indicates that firstly, people are aware of the data that is being collected about them and perceive this as problematic and secondly, the perceived severity of a privacy threatening risk, i.e., users' perception of its seriousness (Witte, 1992), is associated with their protective behavior. Based on this existing literature, we derived the following hypothesis for our study:

H1: Risk awareness is positively associated with internet users' application of self-help strategies to cope with algorithmic risks.

2.3.2 Personal Risk Affectedness and Self-Help Strategies

Furthermore, protective behavior has been theorized to be associated with one's prior experience regarding a risk (Rogers, 1975) as well as the perceived susceptibility to it (Rosenstock, 1974). There is robust empirical evidence for this relationship regarding online risks: several empirical studies have shown that having experienced that one's privacy has been violated or feeling that it could be violated leads to increased levels of privacy protection and an increase in applying privacy-enhancing techniques and technologies when using social media (see Debatin et al., 2009) or the internet in general (see Büchi et al., 2017; H. Chen & Atkin, 2020; Ireland, 2020). Having experienced privacy breaches relates to an increased level of awareness of this risk (Baek et al., 2014; Cho et al., 2010). Deducted from these findings, we propose the following hypothesis:

H2: Personal risk affectedness is positively associated with internet users' application of self-help strategies to cope with algorithmic risks.

2.3.3 Algorithm Skills and Self-Help Strategies

Finally, another aspect that has been found to be central for individual risk protection behavior, is the perceived self-efficacy to cope with a risk (Rogers, 1975; Rosenstock, 1974) or a users' knowledge or skills related to this risk (Montaño & Kasprzyk, 2008). Congruently, findings from several representative survey studies focusing on internet use have shown that users' response-efficacy or self-efficacy is relevant for their protection behavior to reduce risks related to their privacy (Boerman et al., 2018; Dienlin & Metzger, 2016; Ham, 2017). In the same way, users' privacy literacy and internet skills have been shown to be associated with the degree to which they protect their privacy online (Bartsch & Dienlin, 2016; Baruh et al., 2017; Büchi et al., 2017; H. Chen & Atkin, 2020). More recently, besides traditional media literacy and internet skills (Hargittai, 2005; Litt, 2013; van Dijk, 2020), the omnipresence of algorithms in an online environment has led to a specific subset of internet skills coming into the focus of researchers. This specific type of internet skills relates to algorithmic selection and has been referred to as algorithm literacy or algorithm skills (see Dogruel et al., 2021; Gruber et al., 2021; Hargittai et al., 2020). Based on this extant research, we derived the following hypothesis:

H3: Algorithm skills are positively associated with internet users' application of self-help strategies to cope with algorithmic risks.

2.3.4 Path Model of Factors Associated with Self-Help Strategies

Based on the theoretical models and existing empirical research, the introduced hypotheses lead to the following path model of factors associated with self-help strategies to cope with algorithmic risks (see Figure 1).

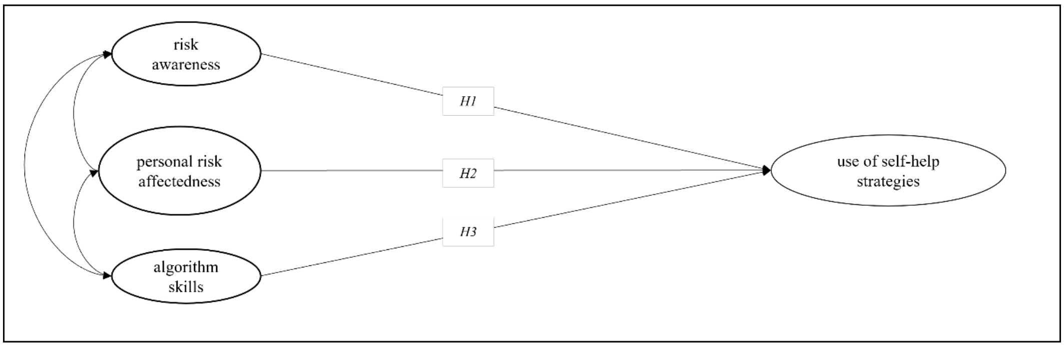

Figure 1. Path Model of Factors Associated with the Application of Self-Help Strategies to Cope with Algorithmic Risks. Source: Own illustration, based on Montano & Kasprzyk (2008), Rogers (1975), and Rosenstock (1974).

2.3.5 Interplay of Factors Associated with Self-Help Strategies

Regarding the relationships between these factors that are associated with self-help strategies to cope with algorithmic risks, we take the general theoretical approaches as a basis. Firstly, the protection motivation theory (Rogers, 1975) proposes that risk awareness correlates with personal risk affectedness and with skills. Secondly, the health belief model (Rosenstock, 1974) suggests that skills correlate with risk affectedness as well. With our model we apply these relationships to the field of algorithmic risks and hence to the awareness of algorithmic risks, the personal affectedness by algorithmic risks, and algorithm skills. Our model reflects these theoretical assumptions as the covariances between risk awareness, personal risk affectedness, and algorithm skills were estimated freely.

In addition to this model, sociodemographic background variables have been conceptualized to play a role as for people's application of protective behavior (Rosenstock, 1974). Previous research has shown that age, gender and the level of educational attainment are related to the awareness of algorithms and associated risks as well as to the level of skills and the application of protecting practices online (Cotter & Reisdorf, 2020; Park, 2011, 2015). At the same time, factors like one's experience with algorithms online (Cotter & Reisdorf, 2020; Swart, 2021) or a person's internet skills (Büchi et al., 2017) were found to be more important in explaining protective behavior than sociodemographic background variables.

2.4 Contributions

By empirically testing the theoretically derived model above, this article contributes to filling the following research gaps. While research on self-help strategies to cope with algorithmic risks is emerging, it has several blind spots. By mainly focusing on one specific application of algorithmic selection (e.g., personalized recommendations, curated social media news feed), or a certain population (e.g., users of one social networking site, youths), previous research offers limited insights into the use of self-help strategies against algorithmic selection for general internet use. Moreover, most of the studies in the field have focused on single influencing factors on risk protection strategies. A more comprehensive analysis of influencing factors and their interplay is wanted. Furthermore, so far, research has predominantly focused on privacy protection practices (e.g., Boerman et al., 2018; Büchi et al., 2017; Ireland, 2020), although the list of risks associated with using algorithmic-selection applications is much more diverse. Further algorithmic risks like surveillance, distorted information, or perceived internet overuse have not been considered thoroughly yet, and accounts on the adoption of strategies to cope with such algorithmic risks are lacking so far. In addition, while recently, qualitative studies on the awareness of algorithms (Dogruel et al., 2020; Hargittai et al., 2020; Swart, 2021) or practices related to data collection (Selwyn & Pangrazio, 2018) were conducted, more generalizable findings and the systematic testing of possible associations are desired. Finally, many of the existing quantitative studies have been conducted in the US. Extending research beyond this context is essential for gaining relevant insights on a societal level. In sum, nationally representative, theory-driven and user-centric empirical studies on how internet users cope with diverse algorithmic risks and what factors play together in being associated with diverse self-help strategies are lacking. We aim to contribute to filling this gap by investigating how awareness of algorithmic risks, personal risk affectedness, and algorithm skills relate to the self-help strategies that users apply to cope with the algorithmic risks of surveillance, distorted information, and internet overuse. The following section describes the methodological design implemented to test the theoretical model introduced above.

3 METHOD

This section details the sample with which the survey was conducted, the measures used, as well as how the data was analyzed.

3.1 Sample

This article analyzes online survey data representative of Swiss internet users aged 16 and over (N_{2018}=1,202) regarding age, gender, household size, and employment status (see Table 1). The data was weighted to closely match the demographics in the general internet-user population. In Switzerland, at the time of data collection, 92% of the population used the internet (Latzer, Büchi, et al., 2019). The sample reflects the three biggest Swiss language regions. Data was collected between November 2018 and January 2019 by an independent market research company. All participants gave informed consent about their participation and the research design was approved by the university's ethics review board.

Table 1. Sample Characteristics. Note. N_{2018}=1,202; Swiss internet users aged 16 and over. Rounded percentages[1].

	Sample
Gender	
female	49%
male	51%
Age	
16-29 years	24%
30-44 years	28%
45-59 years	29%
60-79 years	19%
Education level	
low	7%
medium	67%
high	25%
Household income	
< 6,000 CHF	29%
> 6,000 CHF	71%

3.2 Measures

Central to our analysis are factors associated with the self-help strategies that internet users apply to cope with the algorithmic risks surveillance (*S*), distorted information (*D*) and internet overuse (*O*). Based on theoretical considerations and previous research we identified the following influencing factors on internet users' self-help strategies (see Figure 1): risk awareness (1), personal risk affectedness (2), and algorithm skills (3). For each type of risk, these concepts were measured differently, except for algorithm skills, which were measured consistently among risks[2].

Risk awareness. Respondents were asked how often they think about risks that are associated with algorithmic selection (1-4: *never – often*). These risks include for instance the constant monitoring of internet users (*S*), the danger of distorted information (*D*) or spending too much time online (*O*).

Personal risk affectedness. People were asked to what extent they feel personally affected by a list of online risks *(1-5: do not agree at all – strongly agree*). This includes for instance feeling surveilled online (*S*), feeling confronted with untrue claims online (*D*) or thinking that they are relying too strongly on the internet (*O*).

[1] See federal statistical office https://www.bfs.admin.ch/asset/de/479-2000 for description of the Swiss population.

[2] See https://osf.io/c7aj3/?view_only=5e5343dce34e4486a1d0750642e1577f for exact wordings of all included items.

Algorithm skills. Respondents were asked to indicate their understanding of a list of terms related to the internet and algorithmic selection *(1-5: do not understand the term at all – completely understand the term).* This list included terms like 'algorithm' or 'personalized recommendation' that are related to the internet and algorithmic selection. Its design was adapted from Hargittai (2005), and the list was modified to reflect skills related to algorithms.

Self-help strategies. After having assessed the relevance of a list of risks that can be associated with using the internet, respondents were asked: "There are several things you can do to protect yourself or to deal with such risks. Please indicate how often *(1-5: never – always)* you do the following things". In this way, there were asked about the frequency with which they apply self-help strategies to cope with algorithmic risks. These strategies include adjusting one's privacy settings on certain online services as a strategy to reduce surveillance (S_{strat}), double-checking information online as a strategy to deal with distorted information (D_{strat}) and deliberately ignoring automated recommendations as a strategy to mitigate perceived internet overuse (O_{strat}).

Sociodemographic background. Respondents' gender (1=m, 2=f), age (1=16-29, 2=30-44, 3=45-59, 4=60-79), level of educational attainment (1=low, 2=medium, 3=high), and household income (1=< 6,000 CHF, 2 = > 6,000 CHF) were noted.

3.3 Data Analysis

We calculated a separate SEM using the package *lavaan* in *R* for each algorithmic risk, i.e., surveillance (*S*), distorted information (*D*), and overuse (*O*) to estimate the association of risk awareness (1), personal risk affectedness (2), and algorithm skills (3) with the application of self-help strategies for each of the algorithmic risks. As an estimator, we used maximum likelihood estimation. To deal with missing data, we used full information maximum likelihood estimation. All three measurement models showed an acceptable fit according to Hu and Bentler (1999): for surveillance, the fit indices were χ_S^2=95.977; df_S=24; p<.05; CFI_S=.963; TLI_S=.944; $RMSEA_S$=.050; $SRMR_S$=.034; for distorted information, the fit indices were χ_D^2=115.747; df_D=32; p<.05; CFI_D=.959; TLI_D=.942; $RMSEA_D$=.047; $SRMR_D$=.032; and for overuse, the fit indices were χ_O^2=43.719; df_O=21; p<.05; CFI_O=.974; TLI_O=.960; $RMSEA_O$=.047; $SRMR_O$=.020.

4 RESULTS

This section shows the frequency with which internet users apply the different self-help strategies and presents the results of the SEMs for each algorithmic risk.

Figure 2 depicts the results of the SEM for the algorithmic risk *surveillance (S)*, only displaying significant influencing paths (p<.05).

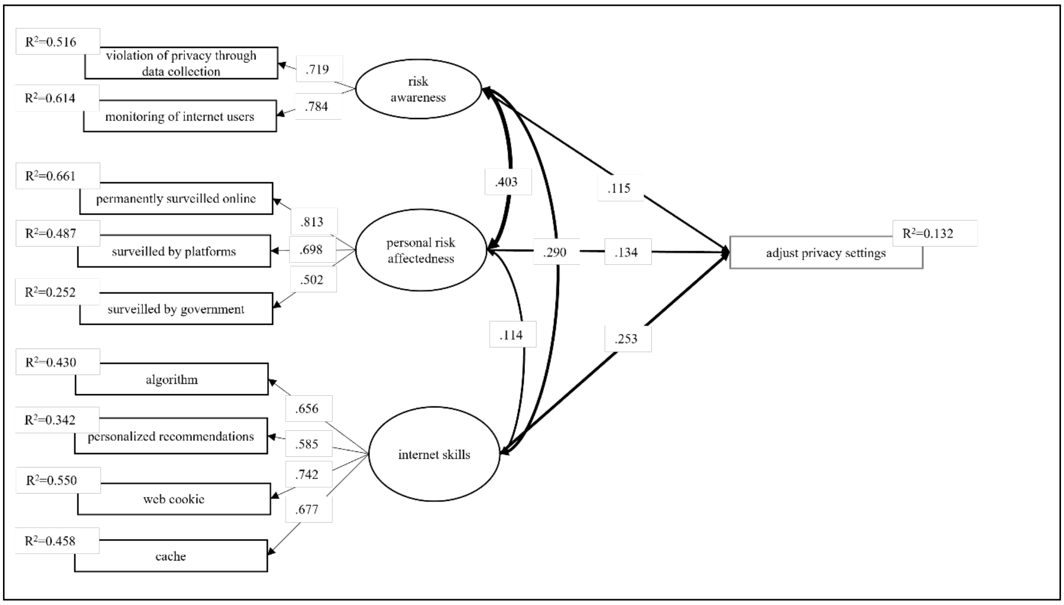

Figure 2. Factors Associated with Internet Users' Application of Self-Help Strategies to Cope with Surveillance. Note. Standardized path coefficients, p<.05; line width of hypothesized effects is scaled to the coefficients. N_{2018}=1,202; Swiss internet users aged 16 and over.

For the risk of surveillance (*S*), the fit indices of the SEM were acceptable according to Hu and Bentler (1999): χ_S^2=113.407; df_S=30; p<.05; CFI_S=.960; TLI_S=.940; $RMSEA_S$=.048; $SRMR_S$=.033. 31% of internet users say that they adjust their privacy settings for certain internet services often or always[3]. The results reveal that this self-help strategy to cope with surveillance is positively associated with risk awareness, with personal risk affectedness and with the level of algorithm skills. Thus, for surveillance, we can accept hypotheses $H1_S$, $H2_S$ and $H3_S$. Furthermore, the covariances of all influencing factors were significant and positive, which is in line with our assumptions introduced above.

Figure 3 depicts the results of the SEM for the algorithmic risk *distorted information (D)*, only displaying significant influencing paths (*p*<.05).

[3] See https://osf.io/c7aj3/?view_only=5e5343dce34e4486a1d0750642e1577f for distribution of frequencies for all self-help strategies.

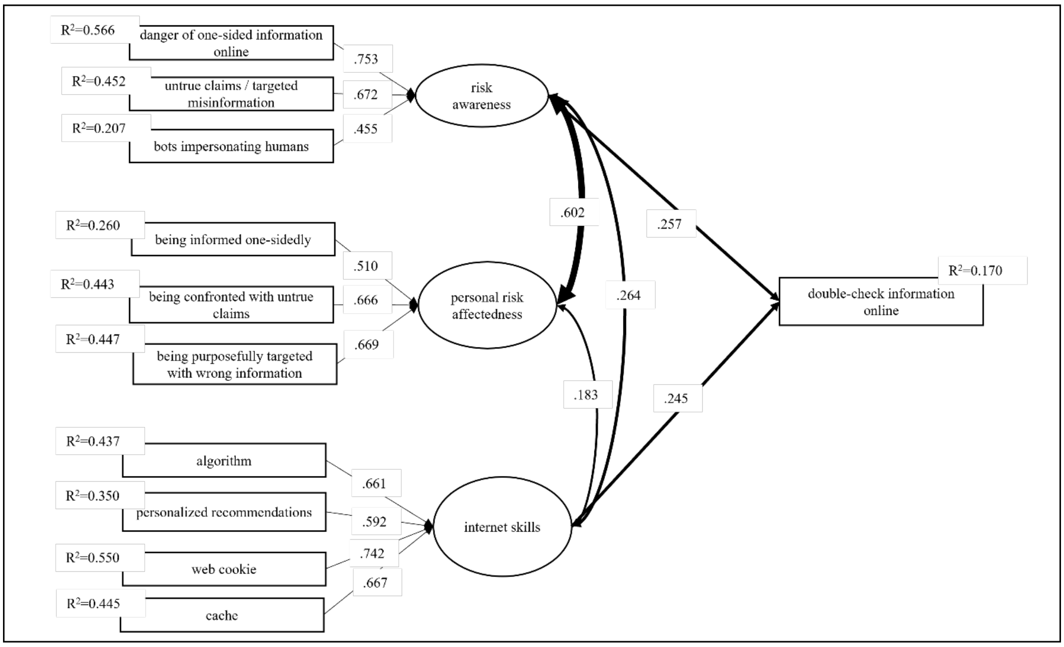
R²=0.566
danger of one-sided information online
R²=0.452
untrue claims / targeted misinformation
R²=0.207
bots impersonating humans
.753
.672
.455
risk awareness
R²=0.260
being informed one-sidedly
R²=0.443
being confronted with untrue claims
R²=0.447
being purposefully targeted with wrong information
.510
.666
.669
personal risk affectedness
.602
.264
.183
.257
.245
R²=0.170
double-check information online
R²=0.437
algorithm
R²=0.350
personalized recommendations
R²=0.550
web cookie
R²=0.445
cache
.661
.592
.742
.667
internet skills

Figure 3. Factors Associated with Internet Users' Application of Self-Help Strategies to Cope with Distorted Information. Note. Standardized path coefficients, p<.05; line width of hypothesized effects is scaled to the coefficients. N_{2018}=1,202; Swiss internet users aged 16 and over.

For the risk of distorted information (*D*), the fit indices of the SEM were also acceptable: $\chi_D 2$=134.552; df_D=39; p<.05; CFI_D=.957; TLI_D=.939; $RMSEA_D$=.045; $SRMR_D$=.032. 46% of internet users state that they often or always double check information online by using additional information sources or different search engines. This self-help strategy to cope with distorted information is positively associated with risk awareness and with the level of algorithm skills, but not with risk affectedness. For the risk of distorted information, we can thus accept $H1_D$ and $H3_D$, but not $H2_D$. Again, the covariances between the influencing factors were significant and positive.

Figure 4 depicts the results of the SEM for the algorithmic risk *internet overuse (O)*, only displaying significant influencing paths (*p*<.05).

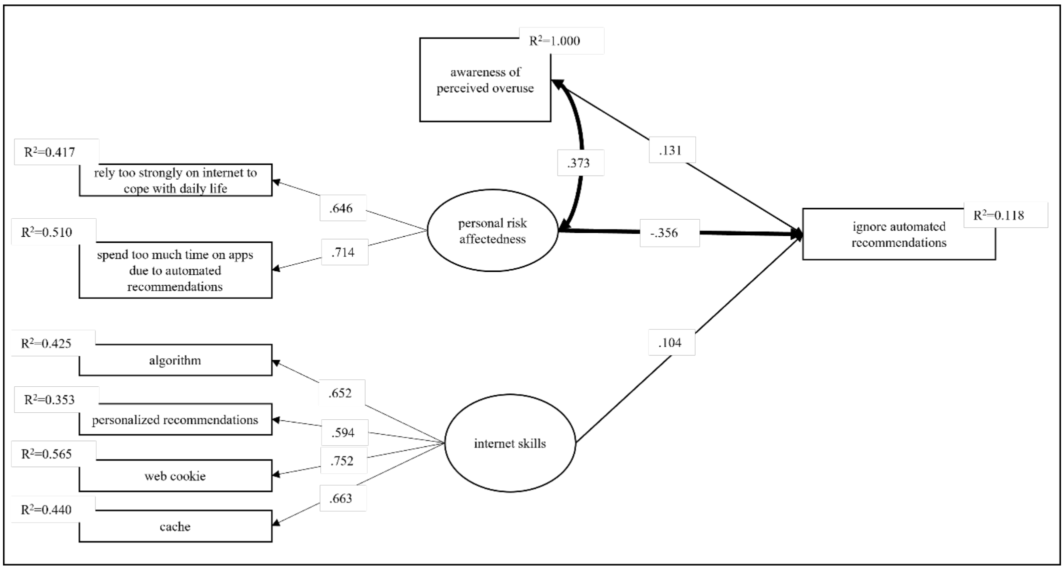
R²=1.000
awareness of perceived overuse
R²=0.417
rely too strongly on internet to cope with daily life
R²=0.510
spend too much time on apps due to automated recommendations
.646
.714
.373
.131
personal risk affectedness
-.356
ignore automated recommendations
R²=0.118
.104
R²=0.425
algorithm
R²=0.353
personalized recommendations
R²=0.565
web cookie
R²=0.440
cache
.652
.594
.752
.663
internet skills

Figure 4. Factors Associated with Internet Users' Application of Self-Help Strategies to Cope with Internet Overuse. Note. Standardized path coefficients, p<.05; line width of hypothesized effects is scaled to the coefficients. N_{2018}=1,202; Swiss internet users aged 16 and over.

For the risk of internet overuse (*O*), the fit indices of the SEM were good as well: χ_O^2=52.389; df_O=16; p<.05; CFI_O=.972; TLI_O=.951; $RMSEA_O$=.044; $SRMR_O$=.020. 71% of internet users say that they often or always ignore automated recommendations. This self-help strategy to cope with internet overuse is positively associated with users' risk awareness and with their algorithm skills. Moreover, ignoring automated recommendations is negatively associated with personal risk affectedness. Hence, for overuse, $H1_O$ and $H3_O$ can be accepted. For $H2_O$ the direction of the effect is opposite to our expectations. In addition, awareness of perceived overuse covaried significantly positively with risk affectedness. There was no significant covariance between algorithm skills and either of the influencing factors.

Alternative models tested the effects of sociodemographic background variables (i.e., gender, age, educational attainment, and income) on risk awareness, personal risk affectedness, and algorithm skills. There were no notable differences in terms of effect sizes and directions as well as significance levels for the hypothesized associations when sociodemographic variables were included, indicating robustness of the models introduced above (Figures 2–4). However, the alternative models' fit was not satisfactory. Therefore, we decided to exclude sociodemographic background variables from our analysis to ameliorate our models' fit[4].

[4] Refer to https://osf.io/c7aj3/?view_only=5e5343dce34e4486a1d0750642e1577f for an overview over the SEMs including sociodemographic background variables.

5 DISCUSSION

The analyses of the SEMs highlight the importance of a higher level of awareness of algorithmic risks (1) and algorithm-specific algorithm skills (3) on the extent to which internet users apply self-help strategies to cope with the algorithmic risks surveillance (*S*), distorted information (*D*), and overuse (*O*). In addition, we found that personal risk affectedness (2) is positively associated with applying self-help strategies to cope with surveillance (*S*), negatively associated with self-help to cope with overuse (*O*), but not associated with self-help to cope with distorted information (*D*). The negative effect for overuse can possibly be explained through an exposure effect, i.e., a desire or need to use the internet extensively (e.g. through professional or private social pressure, see Gui & Büchi, 2019) may lead to experiencing personal risk affectedness like spending too much time on apps due to automated recommendations merely because a lot of time is spent online; needing to use the internet despite this and thus refraining from ignoring automated recommendations is not an unlikely behavior and in line with extant research on perceptions of internet overuse (Büchi et al., 2019).

Moreover, we found that awareness of algorithmic risks (1), personal risk affectedness (2), and algorithm skills (3) have significant and positive covariances with each other in the models for surveillance (*S*) and distorted information (*D*), but not for internet overuse (*O*).

At the same time, the frequency with which internet users apply different self-help strategies varies between types of risks. Overall, only few internet users apply self-help strategies against surveillance and distorted information on a regular basis. Previous research has suggested this for strategies to protect one's privacy in a similar way (see Boerman et al., 2018). On the other hand, ignoring automated recommendations is more widespread. Explanations for this variation can lie in different aspects of internet use. Viewing privacy as contextual integrity (Nissenbaum, 2010) highlights that users' judgement of data being shared differs with regard to context, actors, attributes and transmission principles (Vitak & Zimmer, 2020). Hence, internet users might judge certain self-help strategies regarding specific algorithmic risks more important than others which may lead to a difference in the use of self-help strategies.

Similarly, qualitative research has shown that the awareness of algorithms varies across different services (Swart, 2021). This may relate to the awareness of algorithmic risks and the felt need for applying strategies to cope with them. In addition, the motives for the use of certain services might be associated with users' online behavior. For instance, wanting to or having to use certain algorithmic applications like social media can override the wish for privacy (Quinn, 2016). Moreover, research has indicated that practices that mitigate the effect of algorithmic selection are often deemed too laborious by users (Kormelink Groot & Meijer Costera, 2014; Monzer et al., 2020). This can lead to users not taking advantage of such strategies even if they wished for more agency over the contents that they are shown (Swart, 2021). Thus, the simpleness of use can be an important factor for self-help strategies, just like knowing how to implement such protective practices is (see Büchi et al., 2017). Another reason for not adopting a certain self-help strategy may lie in the habitual use of algorithmic applications. Such habits can be related to the behavior that one engages in (Montaño & Kasprzyk, 2008). For instance, social media users may not consider unfollowing accounts that they are no longer interested in (Swart, 2021). Social media applications are often woven into users' routines so that discontinuation of use would have severe consequences (Dienlin & Metzger, 2016). The different self-help strategies vary in their impact on users' daily internet use. For instance, not using a certain service at all has a different effect on internet use and its consequences than deleting cookies or ignoring recommendations. This may affect the use of such strategies as well, and consequently, users may refrain from applying them in the first place. In addition, research has indicated that internet users do not see the automated data collection and algorithmic analysis thereof as problematic in the first place, as they state that they have nothing to hide (Demertzis et al., 2021). This suggests that in addition to the possibility that individuals are not aware of risks or do not feel affected by risks, they can also take on an attitude of having nothing to hide and thereby not feel a need to apply any strategies to counter possible risks.

Specifically in Switzerland, people may feel rather certain about digital risks as the GDPR from the EU is applied by many corporations that are operating in Switzerland as well. Recent research has shown that the regulatory context of a country can play a role for internet users' felt need to change how they behave because of potential online harms (Strycharz et al., 2022). At the same time, research in Switzerland has shown that only 25% of internet users do not feel exposed to any dangers when they are online. This suggests that there is still some general skepticism towards safety online (Latzer et al., 2021).

Finally, the use of self-help strategies illustrates that while algorithmic-selection applications exert power over their users, the users also have agency to use those platforms to their ends by acting strategically (Bakardjieva, 2005; Ramizo, 2021; Selwyn & Pangrazio, 2018; van Dijck, 2009). The interaction with algorithmic-selection applications can in turn influence the algorithms as in an online environment, humans and algorithms form a recursive loop (Bucher, 2017; Gillespie, 2014). However, users seem to not always be aware of this reciprocated relationship (Swart, 2021). Assigning the responsibility for data protection in algorithmic environments fully to the users is therefore problematic (Baruh & Popescu, 2017).

The theoretical basis of this study roots in psychological concepts originating in the field of health protection behavior (Montaño & Kasprzyk, 2008; Rogers, 1975; Rosenstock, 1974), to derive how users cope with risks online. In the field of privacy protection, the privacy paradox (e.g., H.-T. Chen, 2018; Gerber et al., 2018) and privacy calculus theory (e.g., H.-T. Chen, 2018; Dienlin & Metzger, 2016; Gutierrez et al., 2019) are approaches that try to explain why internet users engage with social media despite potential privacy-related risks. The mechanisms that these theories propose may also inform the analysis of further algorithmic applications that entail similar risks, and therefore, these concepts could be incorporated in future research on algorithmic risk protection in a broader sense.

For this study, there are a few limitations to consider. First, our study includes a variety of theoretically derived and empirically identified factors that are associated with internet users' self-help strategies aimed at reducing algorithmic risks. Besides the factors that we identified based on our theoretical approaches, further factors that could be associated with internet users' self-help strategies are imaginable. For instance, previous research suggests that age, education, and gender may affect online privacy protection (Büchi et al., 2021). In addition, future research could focus on deriving additional potential influencing factors. For example, internet users' actions can be related to their trust in certain websites and services (Pengnate & Sarathy, 2017). The degree of transparency of algorithmic processes may be associated with users' behavior as well (Dogruel et al., 2020; Kemper & Kolkman, 2019). Moreover, besides the described factors, external shocks (Rosenstock, 1974), like privacy scandals made public in the media, may also play a role on the extent to which users apply self-help strategies to protect themselves (Büchi et al., 2022). At the same time, Swart's (2021) qualitative interviews indicate that such scandals can be common knowledge among social media users without leading them to stop using a certain service. Second, we decided to look at three specific risks that relate to algorithmic selection: surveillance, distorted information, and internet overuse. Future studies could include more digital risks, like for instance discrimination through algorithmic selection (Noble, 2018). Third, we looked at self-help strategies against algorithmic risks in general. In the future, such self-help strategies could be investigated in their relative context, for instance with case studies on self-help strategies regarding algorithmic selection on specific platforms like Instagram or context-specific privacy behavior for instance related to online purchases.

6 CONCLUSION

This study identifies factors that are associated with internet users' self-help strategies to cope with algorithmic risks. We found that internet users adjust their privacy settings, double-check information, and ignore automated recommendations to cope with the algorithmic risks of surveillance, distorted information, and internet overuse to varying degrees. The empirical results from our study representative of Swiss internet users showed that their risk awareness (1), their personal risk affectedness (2), and their level of algorithm skills (3) are important influencing factors on internet users' self-help strategies to cope with these algorithmic risks.

Self-help strategies are a valuable mechanism for the reduction of algorithmic risks. They provide a complementary governance option to the existing and emerging governance mix composed of regulation that is issued by state authorities, industry's self-regulation and market solutions. Appropriate statutory regulations and clear guidelines are a prerequisite for the successful and adequate implementation of such complementary self-help strategies that internet users can apply.

This study analyzed the association of three theoretically derived factors with self-help strategies to cope with three types of algorithmic risks that concern internet users in their everyday digital life. It extends extant research about algorithmic risks mostly limited to threats to privacy and contributes to the field of governance of algorithms more broadly. Thereby, it provides an empirical basis for deducting the apt governance mix and assessing the role that users' self-help could play therein to cope with algorithmic risks.

FUNDING STATEMENT AND ACKNOWLEDGMENTS

This research project received funding from the Swiss National Science Foundation (SNF Grant No. 176443). The authors declare that there is no conflict of interest and thank the reviewers for their valuable comments.

REFERENCES

Baek, Y. M., Kim, E., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48–56. https://doi.org/10.1016/j.chb.2013.10.010

Bakardjieva, M. (2005). *Internet Society: The Internet in everyday life.* Sage. http://dx.doi.org/10.4135/9781446215616

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579–596. https://doi.org/10.1177/1461444815614001

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 1–25. https://doi.org/10.1177/0093650218800915

Bozdag, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and Information Technology*, *15*(3), 209–227. https://doi.org/10.1007/s10676-013-9321-6

Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society*, *20*(1), 30–44. https://doi.org/10.1080/1369118X.2016.1154086

Büchi, M., Festic, N., Just, N., & Latzer, M. (2021). Digital inequalities in online privacy protection: Effects of age, education and gender. *Handbook of Digital Inequality*. https://www.elgaronline.com/view/edcoll/9781788116565/9781788116565.00029.xml

Büchi, M., Festic, N., & Latzer, M. (2019). Digital overuse and subjective well-being in a digitized society. *Social Media + Society*. https://doi.org/10.1177/2056305119886031

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

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review*, *36*, 1–15. https://doi.org/10.1016/j.clsr.2019.105367

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Chen, H., & Atkin, D. (2020). Understanding third-person perception about Internet privacy risks. *New Media & Society*, 1–19. https://doi.org/10.1016/j.chb.2017.01.003

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist*, *62*(10), 1392–1412. https://doi.org/10.1177/0002764218792691

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987–995. https://doi.org/10.1016/j.chb.2010.02.012

Cotter, K. (2019). Playing the visibility game: How digital influencers and algorithms negotiate influence on Instagram. *New Media & Society*, *21*(4), 895–913. https://doi.org/10.1177/1461444818815684

Cotter, K., & Reisdorf, B. C. (2020). Algorithmic knowledge gaps: A new horizon of (digital) inequality. *International Journal of Communication*, *14*(0), 21.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Demertzis, N., Mandenaki, K., & Tsekeris, C. (2021). Privacy attitudes and behaviors in the age of post-privacy: An empirical approach. *Journal of Digital Social Research*, *3*(1), 119-152-119–152. https://doi.org/10.33621/jdsr.v3i1.75

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dogruel, L., Facciorusso, D., & Stark, B. (2020). 'I'm still the master of the machine.' Internet users' awareness of algorithmic decision-making and their perception of its effect on their autonomy. *Information, Communication & Society*, 1–22. https://doi.org/10.1080/1369118X.2020.1863999

Dogruel, L., Masur, P., & Joeckel, S. (2021). Development and validation of an algorithm literacy scale for internet users. *Communication Methods and Measures*, 1–19. https://doi.org/10.1080/19312458.2021.1968361

Ebbers, F. (2020). How to protect my privacy? Classifying end-user information privacy protection behaviors. In *Privacy and Identity Management. Data for Better Living: AI and Privacy* (pp. 327–342). https://doi.org/10.1007/978-3-030-42504-3_21

Festic, N. (2020). Same, same, but different! Qualitative evidence on how algorithmic selection applications govern different life domains. *Regulation & Governance*, rego.12333. https://doi.org/10.1111/rego.12333

Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter bubbles, echo chambers, and online news consumption. *Public Opinion Quarterly*, *80*(S1), 298–320. https://doi.org/10.1093/poq/nfw006

Gan, C. (2017). Understanding WeChat users' liking behavior: An empirical study in China. *Computers in Human Behavior*, *68*, 30–39. https://doi.org/10.1016/j.chb.2016.11.002

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gillespie, T. (2014). *The relevance of algorithms. Media Technologies.* https://doi.org/10.7551/mitpress/9780262525374.003.0009

Gruber, J., Hargittai, E., Karaoglu, G., & Brombach, L. (2021). Algorithm awareness as an important internet skill: The case of voice assistants. *International Journal of Communication*, *15*(0), 19.

Gui, M., & Büchi, M. (2019). From use to overuse: Digital inequality in the age of communication abundance. *Social Science Computer Review*, 089443931985116. https://doi.org/10.1177/0894439319851163

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior*, *95*, 295–306. https://doi.org/10.1016/j.chb.2018.09.015

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

Hargittai, E. (2005). Survey measures of web-oriented digital literacy: *Social Science Computer Review*. https://doi.org/10.1177/0894439305275911

Hargittai, E., Gruber, J., Djukaric, T., Fuchs, J., & Brombach, L. (2020). Black box measures? How to study people's algorithm skills. *Information, Communication & Society*, *23*(5), 764–775. https://doi.org/10.1080/1369118X.2020.1713846

Hildebrandt, M. (2008). Defining profiling: A new type of knowledge? In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen: Cross-disciplinary perspectives* (pp. 17–45). Springer Netherlands. https://doi.org/10.1007/978-1-4020-6914-7_2

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Illouz, E. (2008). *Saving the modern soul: Therapy, Emotions, and the culture of self-help*. University of California Press. https://www.jstor.org/stable/10.1525/j.ctt1pp4br

Ireland, L. (2020). Predicting online target hardening behaviors: An extension of routine activity theory for privacy-enhancing technologies and techniques. *Deviant Behavior*, 1–17. https://doi.org/10.1080/01639625.2020.1760418

Islam, A. K. M. N., Laato, S., Talukder, S., & Sutinen, E. (2020). Misinformation sharing and social media fatigue during COVID-19: An affordance and cognitive load perspective. *Technological Forecasting and Social Change*, *159*, 120201. https://doi.org/10.1016/j.techfore.2020.120201

Just, N., & Latzer, M. (2017). Governance by algorithms: Reality construction by algorithmic selection on the Internet. *Media, Culture & Society*, *39*(2), 238–258. https://doi.org/10.1177/0163443716643157

Kemper, J., & Kolkman, D. (2019). Transparent to whom? No algorithmic accountability without a critical audience. *Information, Communication & Society*, *22*(14), 2081–2096. https://doi.org/10.1080/1369118X.2018.1477967

Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, *20*(1), 14–29. https://doi.org/10.1080/1369118X.2016.1154087

Kormelink Groot, T., & Meijer Costera, I. (2014). Tailor-made news. *Journalism Studies*, *15*(5), 632–641. https://doi.org/10.1080/1461670X.2014.894367

Larus, J., Hankin, C., Carson, S. G., Christen, M., Crafa, S., Grau, O., Kirchner, C., Knowles, B., McGettrick, A., Tamburri, D. A., & Werthner, H. (2018). *When computers decide: European recommendations on machine-learned automated decision making* [Technical Report]. Association for Computing Machinery.

Latzer, M., Festic, N., & Kappeler, K. (2020). Awareness of risks related to algorithmic selection in Switzerland. Report 3 from the project: *The significance of algorithmic selection for everyday life: The case of Switzerland*. Zurich: University of Zurich. http://mediachange.ch/research/algosig

Latzer, M., Büchi, M., & Festic, N. (2019). *Internetverbreitung und digitale Bruchlinien in der Schweiz 2019. Themenbericht aus dem World Internet Project—Switzerland 2019*. Universität Zürich. http://mediachange.ch/research/wip-ch-2019

Latzer, M., & Festic, N. (2019). A guideline for understanding and measuring algorithmic governance in everyday life. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1415

Latzer, M., Hollnbuchner, K., Just, N., & Saurwein, F. (2016). The economics of algorithmic selection on the internet. *Handbook on the economics of the internet*. https://www.elgaronline.com/view/edcoll/9780857939845/9780857939845.00028.xml

Latzer, M., & Just, N. (2020). Governance by and of algorithms on the internet: Impact and consequences. In M. Latzer & N. Just, *Oxford research encyclopedia of communication*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228613.013.904

Latzer, M., Saurwein, F., & Just, N. (2019). Assessing policy II: Governance-choice method. In H. Van den Bulck, M. Puppis, K. Donders, & L. Van Audenhove (Eds.), *The Palgrave handbook of methods for media policy research* (pp. 557–574). Springer International Publishing. https://doi.org/10.1007/978-3-030-16065-4_32

Leeder, C. (2019). How college students evaluate and share “fake news” stories. *Library & Information Science Research*, *41*(3), 100967. https://doi.org/10.1016/j.lisr.2019.100967

Litt, E. (2013). Measuring users' internet skills: A review of past assessments and a look toward the future. *New Media & Society*, *15*(4), 612–630. https://doi.org/10.1177/1461444813475424

Longworth, J. (2018). VPN: From an obscure network to a widespread solution. *Computer Fraud & Security*, *2018*(4), 14–15. https://doi.org/10.1016/S1361-3723(18)30034-4

Lowe-Calverley, E., & Grieve, R. (2018). Thumbs up: A thematic analysis of image-based posting and liking behaviour on social media. *Telematics and Informatics*, *35*(7), 1900–1913. https://doi.org/10.1016/j.tele.2018.06.003

Lutz, C., & Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society*, *0*(0), 1–16. https://doi.org/10.1080/01972243.2021.1897914

Marder, B. (2018). Trumped by context collapse: Examination of 'Liking' political candidates in the presence of audience diversity. *Computers in Human Behavior*, *79*, 169–180. https://doi.org/10.1016/j.chb.2017.10.025

Micheli, M., Lutz, C., & Büchi, M. (2018). Digital footprints: An emerging dimension of digital inequality. *Journal of Information, Communication and Ethics in Society*, *16*(3), 242–251. https://doi.org/10.1108/JICES-02-2018-0014

Montaño, D. E., & Kasprzyk, D. (2008). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In K. Glanz, B. K. Rimer & K, Viswanath (Eds.), *Health behavior and health education. Theory, research, and practice*. Jossey-Bass.

Monzer, C., Moeller, J., Helberger, N., & Eskens, S. (2020). User perspectives on the news personalisation process: Agency, trust and utility as building blocks. *Digital Journalism*, *8*(9), 1142–1162. https://doi.org/10.1080/21670811.2020.1773291

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

Noble, S. U. (2018). *Algorithms of oppression.* De Gruyter. https://doi.org/10.18574/nyu/9781479833641.001.0001

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research, 4*(2), 215–236. https://doi.org/10.1177/0093650211418338

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252–258. https://doi.org/10.1016/j.chb.2015.04.011

Pengnate, S. (Fone), & Sarathy, R. (2017). An experimental investigation of the influence of website emotional design features on trust in unfamiliar online vendors. *Computers in Human Behavior*, *67*, 49–60. https://doi.org/10.1016/j.chb.2016.10.018

Petre, C., Duffy, B. E., & Hund, E. (2019). "Gaming the System": Platform paternalism and the politics of algorithmic visibility. *Social Media + Society*, *5*(4), 1–12. https://doi.org/10.1177/2056305119879995

Quinn, K. (2016). Why we share: A uses and gratifications approach to privacy regulation in social media use. *Journal of Broadcasting & Electronic Media*, *60*(1), 61–86. https://doi.org/10.1080/08838151.2015.1127245

Ramizo, G. J. (2021). Platform playbook: A typology of consumer strategies against algorithmic control in digital platforms. *Information, Communication & Society*, 1–16. https://doi.org/10.1080/1369118X.2021.1897151

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health education monographs*. https://doi.org/10.1177/109019817400200403

Ruckenstein, M., & Granroth, J. (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24. https://doi.org/10.1080/17530350.2019.1574866

Sánchez, D., & Viejo, A. (2018). Privacy-preserving and advertising-friendly web surfing. *Computer Communications*, *130*, 113–123. https://doi.org/10.1016/j.comcom.2018.09.002

Saurwein, F., Just, N., & Latzer, M. (2015). Governance of algorithms: Options and limitations. *Info*, *17*(6), 35–49. https://doi.org/10.1108/info-05-2015-0025

Selwyn, N., & Pangrazio, L. (2018). Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data & Society*, *5*(1), 2053951718765021. https://doi.org/10.1177/2053951718765021

Seyfert, R. (2021). Algorithms as regulatory objects. *Information, Communication & Society*, 1–17. https://doi.org/10.1080/1369118X.2021.1874035

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

Swart, J. (2021). Experiencing algorithms: How young people understand, feel about, and engage with algorithmic news selection on social media. *Social Media + Society*, *7*(2), 20563051211008828. https://doi.org/10.1177/20563051211008828

Syvertsen, T. (2020). *Digital detox*. Emerald Publishing Limited. https://books.emeraldinsight.com/page/detail/Digital-Detox/?k=9781787693425

van Dijck, J. (2009). Users like you? Theorizing agency in user-generated content. *Media, Culture & Society*, *31*(1), 41–58. https://doi.org/10.1177/0163443708098245

van Dijk, J. (2020). *The digital divide*. Polity.

Véliz, C. (2020). *Privacy is power*. Bantom Press. /books/1120394/privacy-is-power/9780552177719

Vitak, J., & Zimmer, M. (2020). More than just privacy: Using contextual integrity to evaluate the long-term risks from COVID-19 surveillance technologies. *Social Media + Society*, *6*(3),1–4. https://doi.org/10.1177/2056305120948250

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science*, *1*(1). https://doi.org/10.1515/opis-2017-0002

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

Zarouali, B., Ponnet, K., Walrave, M., & Poels, K. (2017). "Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior*, *69*, 157–165. https://doi.org/10.1016/j.chb.2016.11.050

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.