University of Amsterdam

UvA-DARE (Digital Academic Repository)

No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies

Strycharz, J.; Smit, E.; Helberger, N.; van Noort, G.

DOI
10.1016/j.chb.2021.106750

Publication date
2021

Document Version
Final published version

Published in
Computers in Human Behavior

License
CC BY

Link to publication

Citation for published version (APA):
Strycharz, J., Smit, E., Helberger, N., & van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior*, *120*, [106750]. https://doi.org/10.1016/j.chb.2021.106750

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

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

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

Download date:10 Mar 2023

Computers in Human Behavior 120 (2021) 106750

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: http://www.elsevier.com/locate/comphumbeh

No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies

Joanna Strycharz [a,*], Edith Smit [a], Natali Helberger [b], Guda van Noort [a]

[a] Amsterdam School of Communication Research, University of Amsterdam, Nieuwe Achtergracht 166, 1018 WV, Amsterdam, Netherlands
[b] Institute for Information Law (IViR), University of Amsterdam, Nieuwe Achtergracht 166, 1018 WV, Amsterdam, Netherlands

ARTICLE INFO

Keywords:
Consumer empowerment
Online privacy
Online data collection
Contextual integrity

ABSTRACT

The General Data Protection Regulation (GDPR) introduced in 2018 in the EU aims to give consumers a high degree of control over their data online in order to allow them to protect their privacy. It also puts high transparency requirements for websites that collect and process data. In fact, consumers have to be informed about technical and legal aspects of data collection; this knowledge should empower them to consciously give or withdraw their consent for data collection. The current study investigates the empowering impact of technical and legal knowledge about online data collection within the theoretical framework of the Protection Motivation Theory, the Regulatory Focus Theory, and contextual integrity.

An online experiment in which participants are exposed to a technical or legal knowledge intervention in either commercial or news website context shows that receiving both kinds of information leads to lower threat appraisal. At the same time, having legal knowledge empowers consumers: it positively impacts their coping appraisal and motivation to reject online data collection. The study findings raise questions about the current transparency requirements about data collection and highlight the importance of legal knowledge as well as law enforcement for online privacy protection of consumers.

Currently, we observe a movement towards more consumer empowerment online. In fact, agency of internet users is one of the central objectives of the General Data Protection Regulation (GDPR) introduced in the European Union. This regulation aims at giving consumers a high degree of control over their data online in order to allow them to protect their privacy. At the same time, high requirements are put forward for data controllers and processors to inform consumers (Li, Yu, & He, 2019). They are required to provide consumers with (1) technical information regarding data collection as well as (2) information about their rights. In past research, such information has been portrayed as two dimensions of digital literacy related to privacy protection behaviors (Park, 2011). When more literate, consumers are expected to be empowered to take informed decisions and give or withhold their consent for data collection and processing. However, it remains unclear if the GDPR measures indeed have the intended impact on agency and empowerment of users.

For users, one of the most noticeable changes introduced with the GDPR is the increased number of website notices asking for consent for different types of data collection. Commonly, users are asked if they consent to have so-called cookies placed on their device. Cookies are small text files that are put on users' devices, such as laptops or smartphones, to facilitate the functionality of a website (functional cookies) or to collect profile information which enables for example targeted advertising (tracking cookies) (Smit, Van Noort, & Voorveld, 2014). Websites are required to inform visitors what kind of data they collect by cookies and are obliged to ask consent for all cookies other than functional cookies.

Such cookie notices and consent requests are a good example of the practical implementation of the law. In fact, 62.1% of websites in Europe now display cookie consent notices, 16 percent points more than before the GDPR entered into force (Degeling et al., 2019). However, while these measures are meant to give users control, it is unclear what their impact is. Similarly, while the information requirements are meant to empower consumers to use such functions consciously, their impact has not been systematically investigated. At the same time, from a theoretical perspective we expect that more knowledgeable consumers are more empowered to take protective action (Baruh & Popescu, 2017). Building on past findings we thus identify the need to investigate the impact of technical and legal knowledge on consumer empowerment online and to understand which factors explain whether people are

[*] Corresponding author.
E-mail addresses: j.strycharz@uva.nl (J. Strycharz), E.G.Smit@uva.nl (E. Smit), N.Helberger@uva.nl (N. Helberger), G.vanNoort@uva.nl (G. van Noort).

https://doi.org/10.1016/j.chb.2021.106750
Received 28 July 2020; Received in revised form 23 September 2020; Accepted 14 February 2021
Available online 17 February 2021
0747-5632/© 2021 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

motivated to withhold their consent for having tracking cookies placed on their devices.

Withholding consent for cookies can be seen as a privacy protection measure. Previous studies uncovered several predictors of online privacy protection, including privacy concerns, attitudes, literacy, age and gender (e.g., Baruh, Secinti, & Cemalcilar, 2017; Boerman, Kruikemeier, & Borgesius, 2018). Similarly, Park (2011) investigated digital literacy and concluded that its three dimensions, namely familiarity with technical aspects of the Internet, awareness of common institutional practices, and understanding of current privacy policy, significantly predicted privacy control behaviors such as not visiting certain websites. Similarly, Desimpelaere, Hudders, and Van de Sompel (2020) concluded that knowledge provision in form of privacy literacy training motivates children to take protective measures. As previous studies focused on generic knowledge measures and a limited set of privacy protective behaviors or specifically children population, the current study aims to translate these findings to the GDPR context and investigates what the impact is of the information obligations on internet users' rejection of tracking cookies, and how this impact can be explained.

The GDPR applies to all organizations that collect and process data of EU residents and aims to empower users in general. However, privacy has been concluded to be highly contextual: what shall be treated as private in one context can be treated differently in another (Nissenbaum, 2004). Users' privacy preferences are thus strongly context-dependent (Acquisti, Brandimarte, & Loewenstein, 2015). The same may apply to cookie-enabled data collection: it may matter what kind of website asks users for their consent: is it a commercial organization or a news provider? It is thus crucial to examine consumer empowerment in the context in which data collection takes place.

The overarching aim of the current study is thus to investigate to what extent technical and legal knowledge increase consumer agency in different contexts. More specifically, the current study aims to investigate: 1) to what extent a knowledge intervention based on the GDPR will have an empowering impact when it comes to rejecting tracking cookies[1]; 2) how we can explain the empowerment through knowledge; 3) to what extent the two knowledge types affect consumer motivations and attitudes differently; and 4) to what extent the empowering impact of knowledge depends on context of data collection. To answer these questions, we manipulated the knowledge types mandated in the GDPR and measured user motivations and attitudes. Theoretically, we draw upon the Protection Motivation Theory (PMT) (Rogers, 1975), the Regulatory Focus Theory (RFT) (Higgins, 1997), and the contextuality of privacy (Nissenbaum, 2004). These three theories have been central in studying online privacy issues and behavior (e.g., Boehmer, Larose, Rifon, Alhabash, & Cotten, 2015; Boerman et al., 2018), and past research has shown that providing individuals with knowledge can be seen as a trigger of processes introduced in PMT and RFT (Higgins, 1997; Xiao et al., 2014). Therefore, these theories are combined to explain the empowering impact of knowledge.

Our study makes multiple contributions. Theoretically, it contributes to theory building on how knowledge can contribute to consumer empowerment in the digital sphere. More specifically, the study extends the PMT by the multidimensional construct of knowledge and integrates it with the RTF to explain the potentially empowering impact of technical and legal knowledge. To the best of the knowledge of the authors, PMT and RFT have not been integrated in the consumer empowerment research field. It also adds to past research on protective behavior online by applying the notion of contextuality, which has been widely discussed from the theoretical perspective but often ignored in empirical research. Practically, the study puts the translation of the legal framework to test and offers insights into the actual effects of the GDPR and consumer empowerment measures taken by websites.

1. Theoretical framework

1.1. GDPR and empowerment through knowledge

On May 25, 2018, the GDPR went into effect in the European Union. Its aim is to set high standards across the EU for the collection and processing of personal data (or whenever personal data of EU residents are involved) as well as enhance consumer empowerment and the free flow of data across the Union. As a result, the regulation has had a great impact on millions of companies in Europe, and also beyond Europe, and affects the way how personal data is processed online and what information is disclosed to the users. More specifically, the GDPR impacts how data collection on the web is designed, what data are collected, and how users are informed about these practices (Degeling et al., 2019). For the current study, the requirements of transparency and informed consent for placing cookies are of particular relevance. A more general discussion of the regulation can be found in legal literature (e.g., Greengard, 2018; Tankard, 2016).

Regarding transparency, the GDPR sets high standards for companies to inform consumers about data collection and processing practices, and consumer rights. First, anyone who processes personal data is required to inform users how it takes place (Art. 12). Second, the GDPR mandates websites to inform users about their rights such as Right of Access to Data, Right to Data Portability, and Right to be Forgotten (GDPR, Art. 13 (2)). In addition, the European ePrivacy Directive mandates additional information and consent obligations for the storing or retrieving of information from an end-user's devices, except for so-called strictly necessary cookies (ePrivacy Directive Art. 5(3)). These requirements mean, among others, that every website needs a privacy policy to address these rights.

Similar distinction between different knowledge types has been introduced in the literature by Park (2011). More specifically, he demonstrated that so-called *digital literacy* was multidimensional and consisted of 1) familiarity with technical aspects of the Internet, 2) awareness of surveillance practices, and 3) policy understanding. The GDPR specifically focuses on the awareness of surveillance practices and on policy understanding. Park (2011) concluded that user knowledge strongly predicted privacy control behavior. Along these lines, the knowledge mandated by the GDPR is expected to empower users to make informed decisions regarding consent to data collection using cookies (Degeling et al., 2019).

1.2. Empowering role of technical and legal knowledge

The aim of the European regulator is thus to make sure that consumers have enough knowledge to be able to make informed decisions regarding giving their consent to companies for collecting and processing their personal data, and establish them with concrete rights regarding the way and modalities of data processing. At the same time, past research has concluded that users know little about how their personal data are collected and processed online (Smit et al., 2014). Similarly, internet users have little legal knowledge about their rights. Ur, Leon, Cranor, Shay, and Wang (2012) showed that users did not know how to control data collection online, while Strycharz, Van Noort, Smit and Helberger (2019) concluded that 84% of Google users did not know that they had a possibility to reject data processing by the company. This lack of knowledge impedes user agency: users are not able to take control over their personal data online (Cranor, 2012).

At the same time, in line with the expectations of the regulator, knowledge of an issue itself and knowledge about any recommended protective behavior are an important component for individual motivation to perform such a protective behavior. In the health domain, for example, it has been proven that knowing about a certain illness leads to

[1] Insofar, the focus of the research is on the information obligations under GDPR regarding the use of personal data, and not on additional obligations regarding the storage of information on end-users' equipment under the ePrivacy Directive, which is subject to a pending revision.

higher motivation to perform self-exams (Morman, 2000). Similarly, in privacy research, knowledge is seen as a factor that can equip users with the tools to protect their privacy (Baruh & Popescu, 2017). According to Park (2011), technical knowledge about data flows and knowledge about the legal framework is necessary for users to exercise privacy protection behaviors. These knowledge dimensions reflect the two knowledge types mandated by the GDPR. Applying the past findings to the cookie consent notices context, we expect that receiving both technical and legal knowledge empowers users to action and motivates them to reject cookies. We hypothesize that:

H1. Receiving a) technical and b) legal knowledge intervention about data collection and processing through cookies positively impacts the motivation to reject tracking cookies.

1.3. *Explaining empowerment through knowledge with PMT*

In other domains, the empowerment through knowledge has been commonly explained by protection motivation theory (PMT) (Xiao et al., 2014). PMT was originally developed by Rogers (1975) to explain why people were motivated to protect themselves from health threats. More recently, the theory has been applied to threats online, such as self-disclosure (e.g., Mousavizadeh & Kim, 2015). In the context of this study, the risky behavior can be defined as actions taken online that put one at risk, and protection motivation is the motivation to exercise “specific computer-based actions that consumers take to keep their information safe” (Milne, Labrecque, & Cromer, 2009).

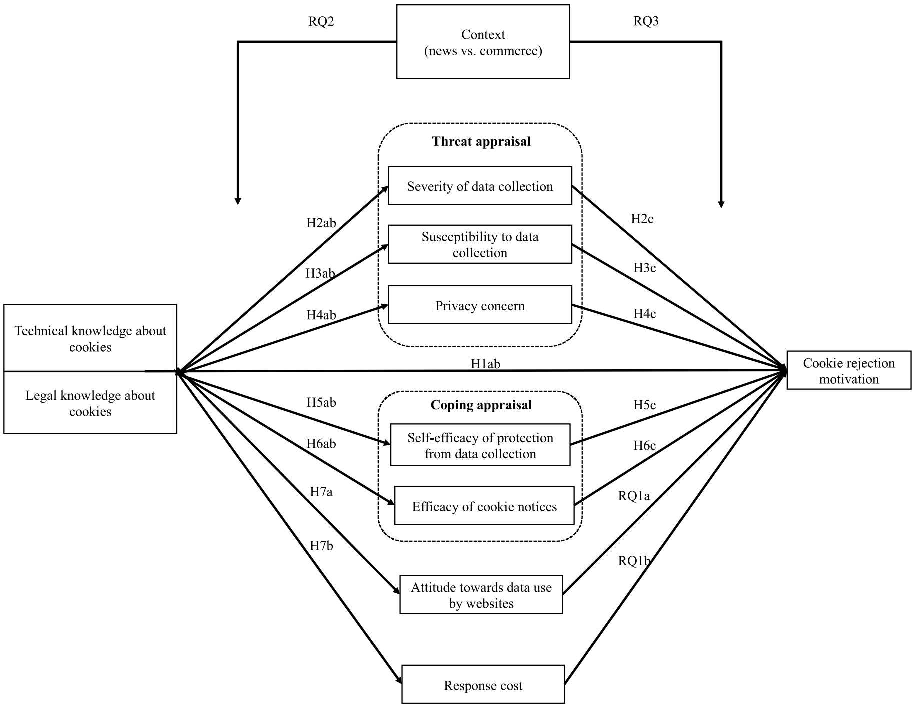
PMT identifies two cognitive processes that motivate a person to act: a *threat appraisal* and a *coping appraisal*. Knowledge has been portrayed as a catalyst of these processes. While the threat appraisal describes one’s belief that the threat is noxious (*perceived severity*) and that it is likely to happen (*perceived susceptibility*), the coping appraisal assesses one’s belief to be able to protect oneself (*perceived self-efficacy*) and that the protective action is effective (*response efficacy*). The theory has been later extended by the *value of the risky behavior* (e.g., attitude towards it or response costs). Furthermore, in the context of privacy behavior online, we argue that an extension of the original theory is necessary and propose that *privacy concern* is vital for the belief that data collection with cookies is noxious. Taken together, the current study tests the empowerment through knowledge model as depicted in *Fig. 1*. In the following sections we further explore the role of threat and coping appraisal as well as the value of the risky behavior for empowerment through knowledge and introduce hypotheses based on PMT.

1.3.1. *Knowledge and threat appraisal activation*

Threat appraisal encompasses two distinct variables: perceived severity and perceived susceptibility. Perceived severity can be defined as one’s judgement about the seriousness of the threat (Rogers, 1975). PMT assumes that individuals who experience a threat as severe are more likely to be motivated to protect themselves from it (Maddux & Rogers, 1983). Indeed, in the health domain, perceived severity has been shown as a trigger of protection motivation (Katz et al., 2009). Similarly, in the privacy protection context, Boerman et al. (2018) concluded that users who see data collection online as problematic are motivated to protect themselves. At the same time, knowledge has been commonly portrayed as a trigger of perceived severity (Xiao et al., 2014). In this study, we expect that consumers who are informed how their data is collected and processed and what rights they have will feel that such practices are a serious issue and will thus be motivated to protect themselves by preventing websites from placing tracking cookies on their devices. Thus, we hypothesize that:

H2. Receiving a) technical and b) legal knowledge intervention about data collection and processing through cookies positively impacts users’ perceived severity and c) perceived severity subsequently positively impacts users’ motivation to reject tracking cookies.

The belief that a threat is severe is, according to PMT, not enough for protection motivation; one also needs to believe that the threat can affect them. Perceived susceptibility describes to what extent an individual feels that it is likely that the threat will happen to them (Rogers, 1975). Past research has shown that it increases one’s motivation to protect themselves from different health threats (Milne, Sheeran, & Orbell, 2000). In the digital context, perceived susceptibility has been described as a driver of motivation to install anti-virus software (Lee, Larose, & Rifon, 2008) or to use pop-up blockers (Boehmer et al., 2015).



RQ2
Context
(news vs. commerce)
RQ3
Threat appraisal
Severity of data collection
Susceptibility to data collection
Privacy concern
H2ab
H3ab
H4ab
H2c
H3c
H4c
Technical knowledge about cookies
Legal knowledge about cookies
H1ab
Cookie rejection motivation
Coping appraisal
Self-efficacy of protection from data collection
Efficacy of cookie notices
H5ab
H6ab
H5c
H6c
H7a
H7b
RQ1a
RQ1b
Attitude towards data use by websites
Response cost

Fig. 1. Hypothesized model. This model illustrates mechanisms behind consumer empowerment through knowledge.

Similarly to perceived severity, in the health context, perceived susceptibility has been driven by knowledge: more knowledgeable individuals start to believe that a threat can affect them (Xiao et al., 2014). Building on past health-related research, we expect that users who are informed how their data is collected and processed and that such collection is regulated by the law, will be more likely to believe that their data may be collected by cookies and thus, they will be more motivated to protect themselves. Therefore, we hypothesize that:

H3. Receiving a) technical and b) legal knowledge intervention about data collection and processing through cookies positively impacts users' perceived susceptibility and c) perceived susceptibility subsequently positively impacts users' motivation to reject tracking cookies.

Finally, we argue that privacy concern is a vital part of threat appraisal in the context of privacy protection online. It can be defined as "concerns about possible loss of privacy as a result of information disclosure" (Xu, Gupta, Rosson, & Carroll, 2012, p. 4). While this construct was not originally included in PMT, its importance has been proven for the data processing context. In particular, Wottrich, van Reijmersdal, and Smit (2018) showed that concerned users refrained from using certain apps, while Milne and Culnan (2004) concluded that it led to more frequent reading of privacy policies. At the same time, knowledge has been regarded as one of the main antecedents of privacy concern. For example, Ermakova, Fabian, Kelkel, Wolff, and Zarnekow (2015) demonstrated that knowledge about technologies was one of the main predictors of health information privacy concern. Along these lines, we expect that consumers who are informed about technical and legal aspects of data collection by cookies will be more concerned about their privacy, which will activate their threat protection and they will be thus more motivated to stop websites from collecting their data. Hence, we hypothesize that:

H4. Receiving a) technical and b) legal knowledge intervention about data collection and processing through cookies positively impacts users' privacy concerns and c) privacy concerns subsequently positively impacts users' motivation to reject tracking cookies.

1.3.2. *Knowledge and coping appraisal activation*

Next to threat appraisal, PMT states that perceptions about protective behaviors are crucial for motivation. First, perceived self-efficacy describes one's belief that they are able to perform the protective behavior (Maddux & Rogers, 1983). In the health domain, self-efficacy has been documented as the strongest predictor of motivation (Milne et al., 2000). In the current study, the concept is used to describe internet users' perceived confidence in preventing companies from collecting their data online. In the online context, research has indeed shown that self-efficacy leads to less self-disclosure (Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009) and to higher motivation to protect oneself, by e.g., installing anti-virus software (Lee et al., 2008). At the same time, receiving knowledge has the power to make consumers more confident in their skills. In fact, in the health context, individuals knowledgeable about an illness felt that they were better able to protect themselves (Xiao et al., 2014). Thus, we expect that knowledge will have the same effect on individuals when it comes to their ability to protect themselves from online data collection through cookies:

H5. Receiving a) technical and b) legal knowledge intervention about data collection and processing through cookies positively impacts users' perceived self-efficacy and c) perceived self-efficacy subsequently positively impacts users' motivation to reject tracking cookies.

Second, perceived efficacy of the protective action is part of the coping appraisal. According to PMT, one needs to believe in effectiveness of an action to be motivated to take it (Maddux & Rogers, 1983). In the health domain, perceived efficacy of the protective action has been shown as an important predictor of protection motivation (see Milne et al., 2000) and recently, this factor has received more attention in the online privacy research. Boerman et al. (2018) have shown the positive impact of response efficacy on different types of online privacy protection, while Strycharz, van Noort, Smit, and Helberger (2019) have concluded that users need to believe in effectiveness of a measure to use it to protect their privacy. At the same time, it is the law enforcement that guarantees the correct working of such protective functions as cookie notices. Similarly, receiving technical knowledge that and how their data is collected and used puts users in the position to be able to ask the follow up-question: how can I protect myself? Thus, we hypothesize that:

H6. Receiving a) technical and b) legal knowledge intervention about data collection and processing through cookies positively impacts users' perceived response efficacy and c) response efficacy subsequently positively impacts users' motivation to reject tracking cookies.

1.3.3. *Knowledge and value of behavior*

Third, the value of the risky behavior has been included in the PMT as a separate element that lowers protection motivation (Maddux & Rogers, 1983). In the original application of the theory in the health context, a meta-analysis shows that indeed, the more the risky behavior is valued and the more negative the response is experienced, the less motivated users are to protect themselves from it (Milne et al., 2000). Regarding data collection, mobile app users who liked an app were found to be less motivated to prevent that app from collecting their data (Wottrich et al., 2018). Similarly, Strycharz, et al. (2019) concluded that positive attitude towards personalized advertising negatively impacted user motivation to opt-out from seeing such ads. Thus, we expect that consumers who enjoy benefits stemming from disclosing their data will be less motivated to reject tracking cookies. At the same time, the cost of the response has been investigated as another crucial construct: when the protective behavior itself causes negative consequences, it also lowers motivation to protect one's privacy (Wottrich et al., 2018). We thus also expect that when rejecting cookies is perceived as something negative, consumers are generally less motivated to do so.

At the same time, relation between the two types of knowledge mandated by the GDPR and attitude towards data collection and response cost is not clear. While the regulator only requires websites to share objective information with visitors, it is not clear if such information fosters positive or negative sides of the phenomenon. We thus hypothesize that consumers who enjoy benefits stemming from their data being collected and used by websites and who perceive rejecting cookies as a burden will be less motivated to reject tracking cookies and pose an open exploratory research question regarding the impact of knowledge:

H7. A) attitude towards data collection and use by websites and b) perceived response cost will be natively related to users' motivation to reject tracking cookies.

RQ1. How does receiving a) technical and b) legal knowledge intervention about data collection and processing through cookies impact one's attitude towards data use by websites and perceived response cost?

1.4. *Two types of knowledge and the PMT*

While PMT explains the mechanism behind the empowering impact of knowledge in general, it does not take its multidimensionality into account. Prior literature on PMT only differentiates between objective knowledge (i.e., what one knows) and subjective knowledge (i.e., what one thinks to know) (Morman, 2000). However, as introduced by Park (2011), objective knowledge in the privacy protection context is multidimensional, which is reflected in the two types of knowledge mandated by the GDPR. One would thus expect that the impact of technical and legal knowledge on threat and coping appraisal differs. We propose to apply the regulatory focus theory (RFT) to better explain the impact of the multidimensional concept of knowledge.

This theory was developed to describe the relationship between one's motivation for goal achievement and the way to achieve the goal (Higgins, 1997). Higgins (1997) specified two frames that motivated individuals to achieve a goal: *promotion focus* associated with characteristics of accomplishment, achievement and aspirations for action, and *prevention focus* associated with security needs, risks, and sensitivity to negative outcomes. Thus, individuals framed into promotion are more sensitive to gains and focused on the desired end-states (in the current study, being able to protect themselves), while individuals framed into prevention are more sensitive to losses and focus on the undesired end-states (in the current study, threat posed by data collection) (Shah, Higgins, & Friedman, 1998). This regulatory focus can be temporarily and situationally induced (Higgins, 1997).

Along these lines, Shih-Chieh Hsu and Shih (2015) proposed an integration of PMT with RFT (see Fig. 2). They argued that previous studies on privacy behaviors largely ignored the fact that, under certain conditions, individuals tend to be more focused on threat or on coping appraisal. To account for this, they proposed that prevention-focused individuals tend to focus on losses and are afraid of the possible negative outcome, which relates to their threat appraisal. At the same time, promotion-focused individuals are more focused on the possible action to approach their ideal goal, which relates to coping appraisal. In the current study, threat appraisal is defined as the perception that the threat to one's privacy is severe and likely to happen, which relates to security risks online, hence it can be expected that prevention focused individuals experience more threat appraisal. At the same time, coping appraisal is defined as the perceived ability to protect oneself from this threat to privacy (by being self-efficacious and having effective protective measures at hand), which relates to taking steps towards the desired state of protection. Hence, it can be expected that promotion focused individuals who aim their attention at the desired protection experience more coping appraisal.

Information provision can activate prevention or promotion focus (Higgins, 1997). In the current study, we assume that legal and technological knowledge interventions are related to prevention (i.e., negative outcomes) and promotion focus (i.e., positive outcomes). More specifically, we apply the reasoning of Shih-Chieh Hsu and Shih (2015) and presume that participants informed about how their data is collected and processed by companies focus on the possible negative outcomes, which is related to threat appraisal, while participants informed about their rights see possibility of action and positive outcomes, which relates to coping appraisal. Thus, integrating PMT and RFT we hypothesize that:

H8. Receiving technical knowledge intervention has a stronger impact on threat appraisal, while receiving legal knowledge intervention has a stronger impact on coping appraisal.

1.5. *Contextuality of privacy protective behavior*

Privacy is context-dependent (Acquisti et al., 2015): information private in one context, may be appropriate to share in another. For example, one discloses different information to their hairdresser than to a healthcare provider. Nissenbaum (2004) has provided the framework of contextual integrity: in order to determine if a specific action violates one's privacy, we have to consider the context in which the data flow takes place. This way, one can identify the contextual norms and expectations at play. An interaction that respects these norms and expectations does not violate one's privacy. Thus, consenting to placing tracking cookies may not only depend on one's knowledge, but also on the context. The final aim of the study is thus to explore the role of context in the empowerment through knowledge mechanisms presented in the previous sections.

In the digital space, e-commerce sites have been collecting and processing data for personalized recommendations and ads for some time now. Consumers are aware of this practice (Bol et al., 2018) and perceive it as beneficial: personalization has been shown to be convenient, allow users to save money and time (Strycharz, van Noort, Smit, & Helberger, 2019). Conversely, in the context of news, data collection by cookies is in the experimentation phase and is commonly associated with negative outcomes (Bol et al., 2018). Most prominently, consumer data is used for personalized distribution of news. This way, news websites hope to achieve higher engagement, increase the time visitor spend on their website and in the end, increase advertising revenues (Anderson, 2011). However, while receiving relevant news may be perceived beneficial (Bol et al., 2018), scholars associate this with the phenomenon of "filter bubble" (Pariser, 2011), which is commonly seen as a negative development.

A number of studies have taken the privacy contextuality into account and provided empirical evidence for the relevance of context for privacy perceptions and related behaviors. For example, Xu, Dinev, Smith, and Hart (2008) showed that certain contexts, among them e-commerce, can negatively impact privacy concerns and risk perceptions. Similarly, Bol et al. (2018) found a small effect of context on consumers weighting benefits and costs when disclosing their information online. More specifically, personalization affected consumers only in the commerce and news and not in the health context. Considering contextuality of privacy, we argue that context has to be considered also

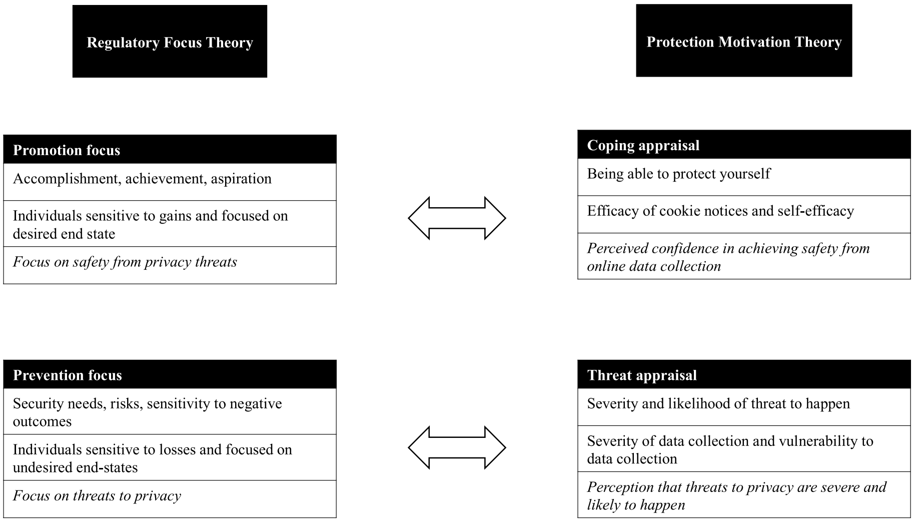

Regulatory Focus Theory
Protection Motivation Theory
Promotion focus
Accomplishment, achievement, aspiration
Individuals sensitive to gains and focused on desired end state
Focus on safety from privacy threats
Coping appraisal
Being able to protect yourself
Efficacy of cookie notices and self-efficacy
Perceived confidence in achieving safety from online data collection
Prevention focus
Security needs, risks, sensitivity to negative outcomes
Individuals sensitive to losses and focused on undesired end-states
Focus on threats to privacy
Threat appraisal
Severity and likelihood of threat to happen
Severity of data collection and vulnerability to data collection
Perception that threats to privacy are severe and likely to happen

Fig. 2. Integration of regulatory focus theory and protection motivation theory.

when investigating the impact of the GDPR-mandated knowledge on user agency and set to explore if empowerment through knowledge is context-specific. Thus, we pose the following exploratory research questions:

RQ2. Does context (i.e., news vs. commerce) moderate the effect of receiving knowledge intervention on threat and coping appraisal as well as attitude?

RQ3. Does context (i.e., news vs. commerce) moderate the relation between threat and coping appraisal and attitude on the motivation to reject tracking cookies?

2. Methods

To test the empowering impact of technical and legal knowledge about data collection online in different contexts, an online experiment was administered, A 3 (knowledge: baseline knowledge vs. baseline + technical data collection knowledge vs. baseline + legal data collection knowledge) x 2 (context: news vs. commerce) in-between subjects design was used.

2.1. Manipulation and stimulus development

Technical and legal knowledge about data collection was manipulated and not just measured, as earlier studies have shown low knowledge and little variation of it among the country's population (Smit et al., 2014). To create external validity, knowledge intervention materials were based on real-world information examples. More specifically, the technical knowledge intervention was based on information provided by the national consumer organization, while the legal intervention was based on information provided by the national Data Protection Authority. The baseline condition introduced the definition of personalization without mentioning cookies as a data collection mode nor technical or legal information. The reading level of the texts was kept at B2 in all conditions. Furthermore, the length of the texts was kept constant in all intervention conditions (technical conditions: 395 words, legal conditions: 404 words), while the baseline conditions were shorter (56 words). In order to manipulate the context, an example was introduced in the manipulation text and throughout the questionnaire. More specifically, participants were told that data collection with cookies happens on for example, news websites such as nu.nl or in for example web shops such as bol.com.

2.1.1. Pretests

First, undergraduate students (N = 91, M_{age} = 22, SD_{age} = 1.86, 77 females) were randomly exposed to one of the three knowledge conditions. The analysis showed that while all texts were equally difficult and professional, the technical text was perceived as more credible than the legal text (F(2, 88) = 3.76, p = .03). Regarding knowledge, participants across the three conditions scored equally well on general knowledge (5 statements), while participants in the technical condition scored significantly higher on technical knowledge (4 statements) compared to participants in general and legal condition (F(2, 88) = 9.95, p < .001). However, participants across three conditions scored equally well on legal knowledge (5 statements). Thus, the manipulation of legal knowledge was not successful. To choose examples for the context manipulation in the main study, at the end of the questionnaire, the participants were asked to rate six largest news sites and web shops on attitude (adopted from Sengupta and Johar, 2002) and familiarity (adopted from Zhou, Yang, and Hui, 2010). Sites with comparable high familiarity (news site: 5.13, web shop: 5.36) and attitude (news site: 4.97, web shop: 5.2) were chosen as examples in the main study.

In the second pretest, we revised the knowledge texts based on errors made by participants in the legal condition and used a national panel with a stratified sampling (N = 156, M_{age} = 53, SD_{age} = 15, 80 females). Analyses showed that while the intervention texts were perceived as equally credible, the baseline text was perceived as less professional (F (2, 125) = 8.93, p < .01), most likely because little information was included. Further, participants across three conditions scored equally well on general knowledge (baseline: M = 3.70, technical manipulation: M = 3.85, legal manipulation M = 3.69), while participants in the technical condition scored significantly higher on technical knowledge (M = 2.54) compared to other conditions (baseline: M = 1.77, legal manipulation M = 2.22; F(2, 118) = 6.68, p < .01) and participants in the legal condition scored significantly higher on legal knowledge (M = 4.31) compared to other conditions (baseline: M = 3.63, technical manipulation: M = 3.79; F(2, 118) = 6.68, p < .01). Thus, in the second pretest the manipulations were successful.

2.2. Participants and procedure

In the main study, we used an online panel from PanelClix to administer the 15-min online survey. Stratification based on age, gender and level of education was applied to make the sample comparable to the general population. From the full responses (N = 658), 284 participants were removed as they failed attention checks, four respondents were removed as they filled in the survey in less than 5 min (indicating inattention), 27 respondents were removed who scored as outliers in completion time (with max of 2.5 h), and 38 participants were removed because they failed the manipulation check for context. Finally, with N = 294, 49% participants were female, M_{age} = 52, SD_{age} = 17.

After reading a factsheet about the study and informed consent, participants were randomly assigned to one of the six conditions. They were asked to carefully read the text and were able to proceed after at least 15 s (baseline texts) or 90 s (manipulation texts). After reading the texts, participants had to answer knowledge questions (manipulation check, same as in the pre-tests). Then, they filled in questions to measure the mediators, dependent variables, and control variables, and a manipulation check asking about the context in the texts. Finally, participants were thanked for their participation and debriefed about the purpose of the study.

2.3. Measures

As a **manipulation check** for knowledge intervention, respondents were asked to answer true/false questions about general data use for personalization (5), about technical (4) and about legal (5) aspects of data collection with cookies. Correct answers were coded 1, and incorrect answers were coded 0. For each scale, the items were summed ($M_{general}$ = 3.86, SD = 1.01; $M_{technical}$ = 1.48, SD = 0.8; M_{legal} = 4.10, SD = 1.00). Regarding context, the respondents were asked what kind of website was referred to in the text with multiple answer options (including "Web-shop such as bol.com" and "News website such as nu.nl"). Respondents answered incorrectly were removed from the sample (34 who chose "No specific website" and 4 who chose the wrong website type).

For our **latent variables**, factor validity was tested via confirmatory factor analyses for each variable separately. In addition, to test discriminant validity and item cross-loadings, we computed an overall model analyzing all variables together. In this model, we allowed parallelly phrased items to covary (measures of susceptibility and severity) with covariances constrained to be equal. According to commonly used fit criteria (e.g., Kline, 2015), all measures showed good model fit and reliability (see Table 1). Some variables violated the assumption of normal distribution and showed heteroscedasticity (see Fig. 3); therefore, we used maximum likelihood estimation with robust standard errors and a Satorra-Bentler scaled test statistic.

Perceived severity was measured with three statements (1 = Strongly disagree, 7 = Strongly agree) derived from Boerman et al. (2018). An example item was: 'Having [web-shops such as bol.com/-news sites such as nu.nl] use cookies to collect information about me online is a problem for me.'

Table 1
Descriptive statistics and factorial validity of all measures.

	M	SD	p(chi^2)	CFI	AIC	RMSEA	Alpha	Omega	Avevar
Perceived severity	5.02	1.37	<.001	1	2855	<.01	.85	.87	.7
Perceived susceptibility	5.29	1.20	<.001	1	2719	<.01	.83	.84	.64
Privacy concerns	4.98	1.24	<.001	1	4311	.04	.91	.91	.67
Self-efficacy	3.66	1.29	<.001	1	2876	<.01	.83	.83	.63
Response efficacy	4.43	1.43	<.001	1	2258	<.01	.96	.96	.88
Response cost	4.06	1.25	<.001	1	3102	<.01	.73	.73	.47
Attitude towards personalization	3.34	1.36	<.001	1	2907	<.01	.83	.84	.64
Overall			<.001	.95	21,749	.06	.85	.87	.69

Note: alpha = internal consistency (Cronbach's alpha); omega = composite reliability (Raykov's omega); avevar = average variance extracted.

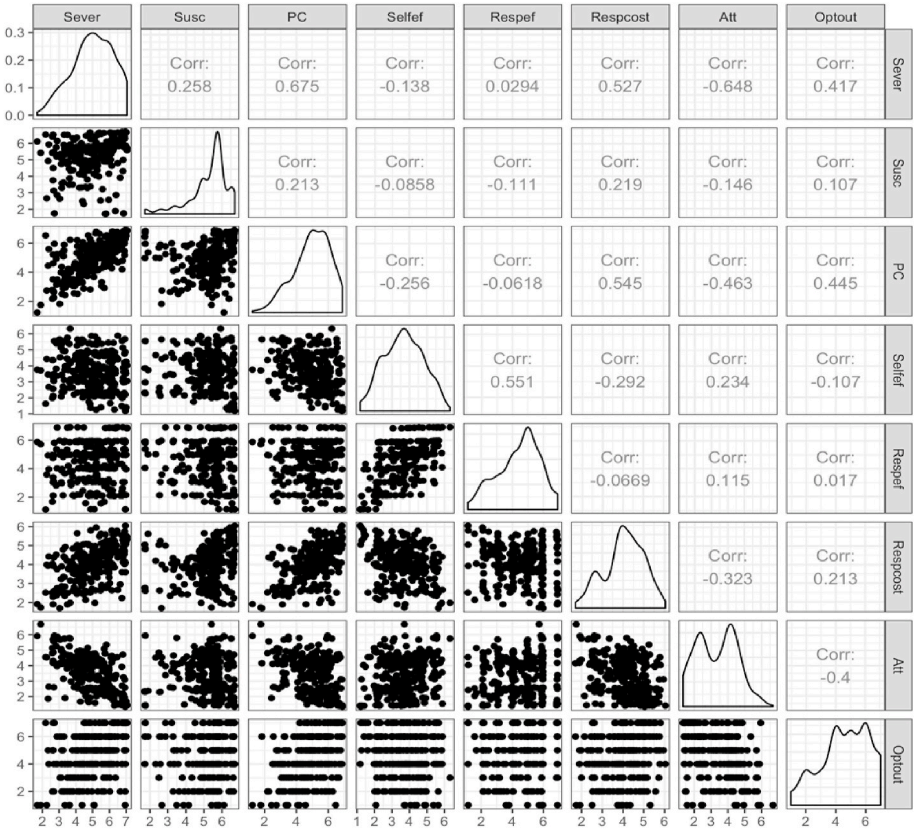


Fig. 3. Variables distribution. This figure illustrates distribution of variables as well as correlations between them. Notes: above diagonal: zero-order correlation matrix; diagonal: density plots for each variable; below diagonal: bivariate scatter plots for zero-order correlations.

To measure the **perceived susceptibility**, we used a three-item scale derived from Boerman et al. (2018) (1 = Strongly disagree, 7 = Strongly agree). An example item was: 'I believe that [web-shops such as bol.com/news sites such as nu.nl] share information about my online behavior with other companies.'

To assess **privacy concerns**, we used a five-item instrument developed by Baek and Morimoto (2012). The scale ranged from 1 (totally disagree) to 7 (totally agree). An example item was: "I am worried that my personal data (such as browsing behavior, name or location) may be misused by [web-shops such as bol.com/news sites such as nu.nl]."

Self-efficacy was measured using three statements (1 = Strongly disagree, 7 = Strongly agree) based on Boerman et al. (2018). An example item was: "I feel confident that I can protect myself online from data collection by [web-shops such as bol.com/news sites such as nu.nl]".

To measure **response efficacy,** we used a three-item instrument derived from Boerman et al. (2018) adopted to focus on efficacy of rejecting tracking cookies. An example item was: "Rejecting cookies is an effective way to protect oneself from data collection online by [web-shops such as bol.com/news sites such as nu.nl]" (1 = Strongly disagree, 7 = Strongly agree).

Response cost was measured by three Likert scale items (1 = Strongly disagree, 7 = Strongly agree) derived from Wottrich et al. (2018), for instance, "Rejecting cookies on [web-shops such as bol.com/news sites such as nu.nl] brings about too many disadvantages for myself."

Attitude towards personalization was assessed with a three-item Likert scale adopted from Tran (2017). An example item was: "I like the idea of [web-shops such as bol.com/news sites such as nu.nl] using my data to show me personalized advertisements and information." (1 = Strongly disagree, 7 = Strongly agree).

Opt-out motivation was measured with one item (1 = very unlikely and 7 = very likely) inspired by Wottrich et al. (2018). The respondents were first shown an example cookie notice (either from a web-shop or a news site) and were presented with the following statement: 'Over the next two weeks, I intend to protect my privacy by rejecting tracking cookies on [web-shops such as bol.com/news sites such as nu.nl]'.

Multiple **control variables** were measured as well. First, we included privacy protection as we expected that other protective behaviors would strongly correlate with our dependent variable, and age and gender as these are factors that influence protection behavior online in the context of knowledge (Park, 2011).

2.4. Data analysis

All variables were analyzed together in multivariate structural equation models (SEM). To test the hypotheses and research questions, we ran separate models for specific analyses (mediation model and between-group SEM). In all models, we controlled for age, and gender, while we also tested that adding privacy protection as a control variable did not change the results (as all three control variables significantly correlated with the motivation to reject cookies). To analyze the impact of context, we compared two groups: news and commerce. First, we tested the SEMs of the respective groups for strict measurement invariance (Kline, 2015), which means that latent factor loadings and item intercepts are equal. Second, we investigated whether the relations differed for the two groups by conducting structural invariance tests (Kline, 2015). This means that if model fit does not decrease significantly after imposing equality constraints on the structural model, the relations between the variables are similar across groups. For the analyses, coding, and typesetting, we used R (Version 3.6.1; R Core Team, 2018) and the R-packages ggplot2 (Version 3.3.0; Wickham, 2016), lavaan (Version 0.6.4; Rosseel, 2012), psych (Version 1.8.12; Revelle, 2018), semTools (Version 0.5.1; Jorgensen, Pornprasertmanit, Schoemann, & Rosseel, 2018), and tidyverse (Version 1.3.0; Wickham, 2017).

3. Results

3.1. Manipulation check

To test the effectiveness of the knowledge interventions, we conducted three ANOVA's with the condition as the independent variable and the three knowledge scores as dependent variables. The results showed that participants across three conditions scored equally well on general knowledge (baseline: M = 4.01, technical manipulation: M = 3.72, legal manipulation M = 3.86); F(2, 291) = 2.1, p = .13), while respondents in the technical conditions scored significantly higher on technical knowledge (M = 1.71) compared to participants in the general (M = 1.33) and legal conditions (M = 1.42) (F(2, 291) = 6.12, p < .01) and participants in the legal conditions scored significantly higher on legal knowledge (M = 4.47) compared to participants in the general (M = 4.03) and technical conditions (M = 3.8) (F(2, 291) = 12.15, p < .01). This confirms that the intervention improved participants' knowledge on the topic.

3.2. Mediation model: impact of knowledge explained through PMT

First, we tested all proposed hypotheses and the first research question (see Fig. 1) in a multivariate mediation model, which showed a good fit ($\chi^2(256) = 425.62$, $p(\chi^2) < 0.00$, CFI = 0.95, RMSEA = 0.05, CI (RMSEA) = [0.04, 0.06]). Regarding H1, we found that the technical (β = −0.03, b = −0.12, z = −0.58, p = .56) nor the legal intervention (β = 0.003, b = 0.01, z = 0.05, p = .96) had a significant direct effect on one's cookie rejection motivation. Hence, participants exposed to the interventions were not directly more or less motivated to opt-out, thereby rejecting H1. H2 proposed the positive mediating role of severity. While we found that receiving technical (β = −0.16, b = −0.48, z = −2.37, p = .02) or legal (β = −0.20, b = −0.59, z = −2.77, p < .001) knowledge intervention significantly decreased one's perceived severity, severity did not have a significant effect on cookie rejection motivation (β = 0.08, b = 0.10, z = 0.86, p = .39) thus rejecting H2. In regards to H3, which proposed the positive mediating role of susceptibility, we concluded a negative effect of technical (β = −0.17, b = −0.48, z = −2.55, p = .01) or legal (β = −0.15, b = −0.40, z = −2.09, p = .04) intervention on perceived susceptibility and no effect of susceptibility on motivation (β = 0.02, b = 0.02, z = 0.30, p = .76). This rejects H3. Next, H4 postulated the mediating role of privacy concerns. We found that neither receiving technical (β = −0.003, b = −0.01, z = −0.04, p = .97) nor legal (β = 0.01, b = 0.03, z = 0.17, p = .86) intervention impacted one's privacy concerns, while privacy concerns did significantly increase one's motivation to opt-out from cookies (β = 0.31, b = 0.40, z = 3.53, p < .001). This partially supports H4 (H4c). Regarding H5, we found that technical intervention did not lead to increased self-efficacy (β = 0.001, b = 0.001, z = 0.01, p = .99), while the legal intervention marginally increased one's self efficacy (β = 0.13, b = 0.27, z = 1.79, p = .07). However, self-efficacy did not have an effect on motivation (β = 0.01, b = 0.01, z = 0.09, p = .93). Thus, H4 is partially supported (H4b). H6 introduced the relation between knowledge intervention, response efficacy and motivation. We concluded that neither technical (β = −0.10, b = −0.30, z = −1.42, p = .16) nor legal (β = 0.07, b = 0.20, z = 1.02, p = .31) intervention impacted response efficacy and that response efficacy did not have an effect on the motivation (β = 0.02, b = 0.02, z = 0.22, p = .82). This rejects H6. Regarding H7, we indeed found a negative relation between attitude towards personalization and motivation (β = −0.20, b = −0.26, z = −2.63, p < .001), while response cost did not significantly impact the motivation (β = −0.07, b = −0.14, z = −0.84, p = .40). This partially supports H7 (H7a). In RQ1 we posed an exploratory question about the impact of receiving knowledge intervention on one's attitude and perceived response cost. We found no significant impact of technical knowledge intervention (β = 0.08, b = 0.22, z = 1.20, p = .23) nor legal knowledge intervention (β = 0.11, b = 0.28, z = 1.46, p = .15) on respondents' attitude. The same applies to response cost (technical knowledge intervention: β = 0.05, b = 0.08, z = 0.62, p = .54, legal knowledge intervention: β = 0.03, b = 0.05, z = 0.38, p = .70).

H8 proposed the difference in impact of technical and legal knowledge on PMT elements. Indeed, while we found no effects on threat appraisal, legal and not technical intervention significantly improved one's perceived self-efficacy partially supporting H8.

3.3. Contexts

Finally, we conducted exploratory analysis if the effect of knowledge intervention on PMT factors differs depending on context (RQ2) and concluded no significant difference in model fit between the structurally constrained model vs. structurally unconstrained model ($\Delta(\chi^2) = 18.33$, Δ(p) = 0.30), which suggests that impact of knowledge intervention on PMT factors did not differ between the two contexts. Similarly, to conclude if the impact of PMT factors on opt-out motivation differs depending on context (RQ3) we compared between-group models and concluded that the fit of structurally constrained model did not differ significantly from the fit of structurally unconstrained model ($\Delta(\chi^2) = 8.02$, Δ(p) = 0.33) indicating that the impact of PMT factors on opt-out motivation did not differ depending on context.

3.4. Additional analysis

We conducted additional analyses with participants' actual scores on technical and legal knowledge scales as independent variables (approach that recently has been suggested in methodological literature as it allows for accounting for differences in manipulation strength, see Breitsohl (2019)). All other model specifications remained the same. The mediation model with knowledge scores as independent variables showed a good fit ($\chi^2(272) = 437.10$, CFI = 0.96, RMSEA = 0.05, CI (RMSEA) = [0.04, 0.06]); Table 2 shows an overview of results for the mediation model. Taken together, higher levels of legal knowledge directly and positively affected cookie-rejection motivation. At the same time, technical and legal knowledge did not significantly affect threat

Table 2
Coefficients for Additional Analyses (mediation model with knowledge scores).

Outcome	Predictor	Coefficient	z-value	p	β
Perceived susceptibility	Technical knowledge	−0.01	−0.02	.98	-.001
	Legal knowledge	−0.27	−0.64	.52	-.04
Perceived severity	Technical knowledge	−0.07	−0.17	.87	-.01
	Legal knowledge	0.07	0.16	.87	.01
Privacy concern	**Technical knowledge**	**−0.61**	**−1.97**	**.05**	**-.13**
	Legal knowledge	0.21	0.56	.58	0.03
Self-efficacy	Technical knowledge	0.02	0.07	.95	.004
	Legal knowledge	**0.77**	**2.61**	< **.01**	**.16**
Response efficacy	Technical knowledge	0.24	0.67	.50	.04
	Legal knowledge	**1.55**	**3.91**	< **.01**	**.22**
Response cost	Technical knowledge	0.19	0.97	.33	.06
	Legal knowledge	−0.05	−0.21	.84	−.01
Attitude towards personalization	Technical knowledge	0.11	0.36	.72	.02
	Legal knowledge	**−0.06**	**−1.65**	**.09**	**−.10**
Optout motivation	Technical knowledge	−0.33	−0.97	.33	−0.05
	Legal knowledge	**1.47**	**3.20**	< **.01**	**.18**
	Perceived susceptibility	0.02	0.26	0.79	.02
	Perceived severity	0.15	1.38	.17	.13
	Privacy concern	**0.35**	**3.22**	< **.01**	**.27**
	Self-efficacy	−0.04	−0.34	.73	−.03
	Response efficacy	0.01	0.09	.93	.01
	Response cost	−0.12	−0.72	.47	−0.06
	Attitude towards personalization	**−0.22**	**−2.08**	**.04**	**−.16**

Notes: significant and marginally significant relations are marked in bold.

appraisal, while technical knowledge decreased respondents' privacy concerns. Regarding coping appraisal, legal knowledge significantly increased respondents' perceived self- and response efficacy. Finally, regarding PMT, similarly to the previous analysis, privacy concern significantly increased motivation, while attitude towards personalization significantly decreased it.

4. Discussion

The aim of this research was to examine impact of GDPR obligations on consumer empowerment, and more specifically the effect of technical and legal knowledge on internet users' motivation to reject tracking cookies, and the underlying processes. The experiment in which users were exposed to a technical or legal knowledge intervention demonstrated that the interventions did not have the expected empowering effect. In fact, we found a negative effect for both interventions on perceived severity and susceptibility. The legal knowledge intervention only had the expected empowering effect with regard to perceived self-efficacy. Also, while not triggered by knowledge, some elements of PMT explained why consumers were (not) motivated to reject tracking cookies. However, when considering objective level of knowledge that users had after the knowledge intervention, findings showed the expected positive effect on coping appraisal and on cookie rejection motivation.

The lack of an empowering effect of the knowledge interventions is unexpected, as PMT and past research on consumer empowerment suggest a positive effect (Xiao et al., 2014). Even more surprising is that findings are more in line with our expectations when analyzing effects of consumers' actual knowledge, instead of the intervention effects. This inconsistency has a few possible explanations and implications for empowerment through knowledge. In fact, PMT prescribes objective knowledge and not the increase in knowledge as a catalyst of threat and coping appraisal. It is thus likely that specifically legal intervention at the same time empowered consumers and induced negative "side-effects": it increased consumers' objective knowledge, and negatively impacted threat appraisal. Threat appraisal was generally high among participants; thus, it is possible that consumers were so negative and "scared" that the knowledge we offered in the intervention gives them a feeling of safety and control. From this perspective, the negative effect on threat appraisal is in line with past research on privacy seals, demonstrating that such seals make users feel more secure (Van Noort, Kerkhof, & Fennis, 2008). Along these lines, in the context of online disclosure, Brandimarte, Acquisti, and Loewenstein (2013) introduced the notion of a control paradox: control over sharing private information increases the willingness to publish sensitive information. The current study suggests that this paradox also takes place in the context of transparency about cookies – receiving such information decreases one's perception of threat. From the perspective of the GDPR we can conclude that offering in particular legal knowledge in itself makes consumers more confident about their protection skills (self-efficacy), but the transparency also has unexpected side-effects that may put consumers' vigilance to sleep and push them towards taking more risks.

For technical knowledge specifically, we may conclude the following. According to PMT and RFT we expected that such knowledge would increase consumers' coping appraisal and would have even stronger effect on threat appraisal (Higgins, 1997; Rogers, 1975). We did not observe these effects. It has to be noted that in general, threat appraisal was high –the scores for perceived severity and susceptibility were above the midpoint of the scale. Thus, ceiling effects may explain the unexpected negative effects.

The GDPR also prescribes information obligations about consumer rights. As discussed above, offering participants such legal knowledge had negative effects on their empowerment. However, objective level of legal knowledge had the expected positive effect on consumer empowerment, i.e. their coping appraisal. In fact, in line with PMT and RFT (Higgins, 1997; Rogers, 1975), higher level of legal knowledge had a positive effect on coping appraisal, while it did not impact threat appraisal. Hence, having more legal knowledge does not automatically result in a change in view on data collection, but it empowers consumers to feel self-efficacious and it makes them believe in the effectiveness of cookie opt-out notices. This confirms that possessing objective legal knowledge is powerful: it raises confidence in skills, which has been proven before in the health context (Xiao et al., 2014). This shows the importance of law enforcement – effective enforcement of the GDPR that guarantees the correct working of cookie notices is important for consumers to believe in the effectives of legal rules. For future research we advocate a stronger focus on consumer faith in the law and law enforcement and its effects on protective behavior.

For PMT we conclude that it only partially explains cookie rejection motivation. Our study found that only two factors from the theory significantly predicted the rejection motivation as expected, namely privacy concern and attitude. In line with past research, privacy concern is the strongest predictor of motivation to opt-out (Milne & Culnan, 2004; Wottrich et al., 2018), and attitude towards personalization negatively affects this motivation (Wottrich et al., 2018). Indeed, past research has shown that people engage in the threat-related behavior in exchange for convenience, functionality, or financial gains (Acquisti & Grossklags, 2005). At the same time, it is surprising that neither threat appraisal nor coping appraisal had the expected effects. The lack of evidence for an effect of perceived susceptibility may be explained by the low variance in this construct: Almost all people believe that their personal information is being collected via tracking cookies, possibly causing a ceiling effect.

For context dependency of privacy (Nissenbaum, 2004) we conclude that it does not apply to the current research context. There was a lack of differences between commerce and news context, suggesting that the effect of particularly legal knowledge on PMT processes, as well as the application of PMT to cookie rejection is stable across industries. It does not matter if a web shop or a news website asks to place cookies, it only matters how concerned one is about their privacy and how much one likes to receive personalized ads and recommendations. Simultaneously, it is worth noting that while context is theoretically an important aspect in studying privacy behaviors, the effects of contextuality of privacy and personalization found in the past have been small so possibly too small to be substantial and to be detected in our study (Bol et al., 2018).

4.1. Limitations and future directions

Despite the intriguing findings the current study has some limitations that also provide interesting directions for future research. First, the protective behavior in the current study, namely rejection of tracking cookies, is only one example of protective behaviors that users can exercise. In fact, while cookies are still the most common way to collect data for e.g., personalized advertising, companies are exploring new forms of collecting information, other than cookies. To what extend users understand and know how to protect themselves from such new ways of collecting data presents an avenue for future research.

Further, the knowledge intervention in the current study was successful in significantly increasing consumer technical and legal knowledge, but its effects were surprising and different than the effect of one's actual knowledge level. In the discussion, we offer a number of explanations, such as inducing a feeling of security or the control paradox. However, one more possible explanation relates to the manipulation itself. The knowledge intervention was the same for every participant, while they had different levels of knowledge before taking part in the study. Some, who closely follow the news, may have learned about technical details behind data collection via cookies and about their rights as such topics have received substantial attention in mass media (Strycharz, van Noort, Smit, Vliegenthart, & Helberger, 2017). Legal knowledge in itself is a successful empowerment factor. However, in order to make use of it and to design successful interventions, one has to consider the knowledge level of the target group and personalize the intervention accordingly.

In addition, technical knowledge was least improved by our intervention: even in the technical intervention condition, the average score was just at the midpoint of the scale. Also, technical knowledge level across the three conditions was lower compared to general and legal knowledge. This suggests that technical information is most challenging for consumers. Past research on knowledge interventions informs us that for complex information visual material is more effective than textual material (Meppelink, Van Weert, Haven, & Smit, 2015). Therefore, for future research on empowerment through knowledge we suggest that interventions should be designed taking into account the complexity of information.

The current study carries a number of implications for organizations that apply personalization and use cookies to collect data as well as for regulators. From an organizational perspective, an important learning is that consumers are afraid and pessimistic (as demonstrated by the high threat appraisal and negative attitudes). Although, consumer's negativity did not translate in a higher opt-out motivation, negative attitudes may negatively influence more long-term outcomes, such as consumer reflections on personalization strategies. The findings also cast doubts on the role of technical transparency. Neither the intervention nor the level of technical knowledge significantly impacted motivation to reject cookies. This is good news for marketers who commonly dread the transparency requirements: purely being informed about how your data is collected, stored and processed does not cause negative attitudes.

From the regulator's viewpoint, the impact of legal knowledge is crucial. The GDPR information obligations with regard to consumer rights do have an empowering effect. However, informing consumers about their rights puts their vigilance to sleep and makes them less concerned, which could be an argument for a more paternalistic approach to privacy protection online, such as privacy nudges as argued for in recent legal research (Soh, 2019), or more stringent forms of command-and-control rules (e.g. bans on certain PMT practices). When designing interventions aimed at increasing consumer knowledge, a number of factors need to be considered. Such interventions need to be adjusted to the level of pre-existing knowledge of the target group, as between audiences (e.g., age in this study) knowledge may differ. Thus, the target group for knowledge interventions needs to be carefully defined to assure consumer empowerment.

Credit author statement

Conceptualization: Joanna Strycharz, Guda van Noort, Edith G. Smit, Natali Helberger. Methodology: Joanna Strycharz, Guda van Noort, Edith G. Smit, Natali Helberger. Data collection: Joanna Strycharz. Analysis: Joanna Strycharz. Writing (original draft presentation): Joanna Strycharz. Writing (review and editing): Joanna Strycharz, Guda van Noort, Edith G. Smit, Natali Helberger. Visualisation: Joanna Strycharz.

Acknowledgments

This research was funded by and made possible through the University of Amsterdam Research Priority Area 'Personalized Communication' (uva-icds.net), as well as through the support of the Stichting Wetenschappelijk Onderzoek Commerciële Communicatie (SWOCC).

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221). https://doi.org/10.1126/science.aaa1465

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine, 3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Anderson, C. (2011). Between creative and quantified audiences: Web metrics and changing patterns of newswork in local US newsrooms. *Journalism: Theory, Practice & Criticism, 12*(5), 550–566. https://doi.org/10.1177/1464884911402451

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

Baek, T. H., & Morimoto, M. (2012). Stay away From me. Examining the determinants of consumer avoidance of personalized advertising. *Journal of Advertising, 41*(1), 59–76. https://doi.org/10.2753/JOA0091-3367410105

Boehmer, J., Larose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology, 34*(10), 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448

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

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

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Breitsohl, H. (2019). Beyond ANOVA: An introduction to structural equation models for experimental designs. *Organizational Research Methods, 22*(3), 649–677. https://doi.org/10.1177/1094428118754988

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communications, 52*(2), 167–182. https://doi.org/10.1109/TPC.2009.2017985

Cranor, L. F. (2012). Can users control online behavioral advertising effectively? *IEEE Security and Privacy Magazine, 10*(2), 93–96. https://doi.org/10.1109/MSP.2012.32

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy ... Now take some cookies: Measuring the GDPR's impact on web privacy. In *NDSS 2019*. https://doi.org/10.14722/ndss.2019.23xxx. San Diego.

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behaviour. *Computers in Human Behavior, 110*. https://doi.org/10.1016/j.chb.2020.106382

Ermakova, T., Fabian, B., Kelkel, S., Wolff, T., & Zarnekow, R. (2015). Antecedents of health information privacy concerns. *Procedia - Procedia Computer Science, 63*, 376–383. https://doi.org/10.1016/j.procs.2015.08.356

Greengard, S. (2018). Weighing the impact of GDPR. *Communications of the ACM, 61*(11), 16–18.

Higgins, E. T. (1997). Beyond pleasure and pain. *American Psychologist, 52*(12), 1280–1300. https://doi.org/10.1037/0003-066x.52.12.1280

Jorgensen, T. D., Pornprasertmanit, S., Schoemann, A. M., & Rosseel, Y. (2018). *semTools: Useful tools for structural equation modeling*.

Katz, M. L., Heaner, S., Reiter, P., van Putten, J., Murray, L., McDougle, L., et al. (2009). Development of an educational video to improve patient knowledge and communication with their healthcare providers about colorectal cancer screening. *American Journal of Health Education, 40*(4), 220–228. https://doi.org/10.1901/jaba.2009.40-220

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

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445–454. https://doi.org/10.1080/01449290600879344

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management, 22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

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

Meppelink, C. S., Van Weert, J., Haven, C. J., & Smit, E. G. (2015). The effectiveness of health animations in audiences with different health literacy levels: An experimental study the Effectiveness of Health Animations in Audiences with Different Health Literacy Levels: An Experimental Study. *Journal of Medical Internet Research, 17*(1). https://doi.org/10.2196/jmir.3979

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29. https://doi.org/10.1002/dir.20009

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Morman, M. T. (2000). The influence of fear appeals, message design, and masculinity on men's motivation to perform the testicular self-exam. *Journal of Applied Communication Research, 28*(2), 91–116. https://doi.org/10.1080/00909880009365558

Mousavizadeh, M., & Kim, D. J. (2015). A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory. *International Conference on Information Systems*, 1–20.

Nissenbaum, H. (2004). *Privacy as contextual integrity. Washington law review*.

Van Noort, G., Kerkhof, P., & Fennis, B. M. (2008). The persuasiveness of online safety cues: The impact of prevention focus compatibility of Web content on consumers' risk perceptions, attitudes, and intentions. *Journal of Interactive Marketing, 22*(4), 58–72. https://doi.org/10.1002/dir.20121

Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. New York, NY: Penguin.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. https://doi.org/10.1177/0093650211418338

R Core Team. (2018). *R: A language and environment for statistical computing*. Vienna, Austria: R Foundation for Statistical Computing.

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

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software, 48*(2), 1–36.

Sengupta, J., & Johar, G. V. (2002). Effects of inconsistent attribute information on the predictive value of product attitudes: Toward a resolution of opposing perspectives. *Journal of Consumer Research, 29*(1), 39–56. https://doi.org/10.1086/339920

Shah, J., Higgins, E. T., & Friedman, R. S. (1998). Performance incentives and means: How regulatory focus influences goal attainment. *Journal of Personality and Social Psychology, 74*(2), 285–293. https://doi.org/10.1037/0022-3514.74.2.285

Shih-Chieh Hsu, J., & Shih, S.-P. (2015). When does one weight threats more? An integration of regulatory focus theory and protection motivation theory. In *Proceedings of the 10th pre-ICIS workshop on information security and privacy* (pp. 12–13).

Smit, E. G., Van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior, 32*, 15–22. https://doi.org/10.1016/j.chb.2013.11.008

Soh, S. Y. (2019). Privacy nudges: An alternative regulatory mechanism to 'informed consent' for online data protection behaviour. *European Data Protection Law Review, 5*(1), 65–74. https://doi.org/10.21552/edpl/2019/1/10

Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019a). Consumer view on personalized advertising: Overview of self-reported benefits and concerns. In *Advances in advertising research X* (pp. 53–66). Wiesbaden: Springer Gabler. https://doi.org/10.1007/978-3-658-24878-9_5.

Strycharz, J., Van Noort, G., Smit, E., & Helberger, N. (2019b). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 13*(2). https://doi.org/10.5817/CP2019-2-1

Strycharz, J., van Noort, G., Smit, E., Vliegenthart, R., & Helberger, N. (2017). Media effects on public opinion about online privacy. In *IC2S2* (Cologne, Germany).

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

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

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy. In *Proceedings of the eighth symposium on useable privacy and security - SOUPS '12* (p. 1). New York, New York, USA: ACM Press. https://doi.org/10.1145/2335356.2335362.

Wickham, H. (2016). *Ggplot2: Elegant graphics for data analysis*. Springer-Verlag.

Wickham, H. (2017). *Tidyverse: Easily install and load 'tidyverse' packages*. https://CRAN.R-project.org/package=tidyverse.

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). App users unwittingly in the spotlight: A model of privacy protection in mobile apps. *Journal of Consumer Affairs*. https://doi.org/10.1111/joca.12218

Xiao, H., Li, S., Chen, X., Yu, B., Gao, M., Yan, H., et al. (2014). Protection motivation theory in predicting intention to engage in protective behaviors against schistosomiasis among middle school students in rural China. *PLoS Neglected Tropical Diseases, 8*(10). https://doi.org/10.1371/journal.pntd.0003246

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual' s privacy concerns: Toward an integrative view. In *ICIS 2008* (Paris).

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In *Thirty third international conference on information systems* (Orlando).

Zhou, L., Yang, Z., & Hui, M. K. (2010). Non-local or local brands? A multi-level investigation into confidence in brand origin identification and its strategic implications. *Journal of the Academy of Marketing Science, 38*(2), 202–218. https://doi.org/10.1007/s11747-009-0153-1