

# Nuisance Letters? E-Mail Newsletters, Privacy, and the Market for Data

*Completed Research Full Paper*

**Katharina Hartinger**

Johannes Gutenberg University Mainz  
khartinger@uni-mainz.de

**Emmanuel Syrmoudis**

Technical University of Munich  
emmanuel.syrmoudis@tum.de

**Alexander Wolfram**

Cath. University of Eichstätt-Ingolstadt  
alexander.wolfram@stud.ku.de

**Maximilian J. Frank**

Technical University of Munich  
maximilian.j.frank@tum.de

**Jens Grossklags**

Technical University of Munich  
jens.grossklags@in.tum.de

This is the Author Accepted Manuscript (AAM) of an article published in the *Proceedings of the Thirtieth Americas Conference on Information Systems (AMCIS)*. The Version of Record is available online at: [https://aisel.aisnet.org/amcis2024/sig\\_hci/sig\\_hci/8](https://aisel.aisnet.org/amcis2024/sig_hci/sig_hci/8)

## Abstract

We study the market for data in the context of online retail newsletters, where consumers sell data in exchange for a discount. On the firm side, data on over 2,000 firms show a convergence towards a 5-10% discount equilibrium. Focusing on the user side, we conduct a survey with over 500 participants where we find substantial heterogeneity among consumers with respect to newsletter preferences and strategies. When we vary nuisance and privacy as key newsletter characteristics in a vignette experiment, the share of consumers who demand a higher-than-usual discount for subscription increases significantly when privacy is low—although actual subscription behavior remains unchanged. Allowing consumers to interact with a privacy tool to analyze real-world newsletters sparks substantial engagement and interest among survey participants: 63% choose to analyze more newsletters than they had originally been assigned. Our findings call for more accessible information on newsletter features.

## Keywords

Newsletters, market for data, privacy, email marketing, consumer reaction.

## Introduction

An online shopping experience rarely comes without a newsletter subscription pop-up these days: “Simply enter your personal data to get 10 percent off your first order!” In this paper, we study consumer interactions with newsletters in a survey experiment to shed light on the market for consumer data in the context of email marketing. Specifically, we focus on two characteristics of newsletters: Their level of nuisance and their degree of privacy intrusion through data collection.

Email newsletters are a popular marketing tool in online retail to increase customer loyalty through communication (Cases et al. 2010). Beyond marketing, however, they provide a largely understudied setting for

human-computer interaction research with two particularly intriguing features: First, the market-for-data equilibrium is *explicit* in the context of newsletters since we find that a majority of companies offer discounts in the 5 to 10% range in exchange for consumer data, which can be considered the equilibrium price for the bundle of information (such as email address, other personal data, and preferences) and access (the ability to send messages directly to the consumer). Second, compared to other privacy-related decisions (such as whether or not to sign up for a social network), newsletter sign-up is a rather casual, frequent, and organic decision and, therefore, adds to our overall understanding of everyday consumer behavior online. But these subtle subscription decisions are not necessarily innocent. The literature dedicated specifically to email marketing highlights negative consequences of subscribing, such as involuntary or nontransparent tracking (Englehardt et al. 2018; Kalantari et al. 2021) or extensive personalizing (White et al. 2008).

Thus, with nuisance and privacy as the defining elements of interest, we conduct a survey experiment with 527 students at a large German university to investigate how consumers react to newsletter characteristics in their subscription decision. Specifically, we address the following three research questions:

**RQ1:** What are the characteristics of the market for newsletter subscriptions? The consumer's (equilibrium) willingness to accept a discount (WTA) is a key determinant of the market equilibrium and, thus, a central outcome of our analyses that connects the different research questions.

**RQ2:** How do consumers react to the design of newsletter subscription forms with regard to their subscription decision, expectations about newsletter quality, and required compensation for subscription?

**RQ3:** How do consumers react when they are given the opportunity to analyze the privacy characteristics of real-world newsletters with a tool?

These three core research questions call for a survey design strategy where we combine descriptive survey evidence (to explore participants' preferences and self-reported behaviors) with a vignette study to explore causality. We document substantial heterogeneity in the number of newsletter subscriptions (around an average of 7.4) as well as in the minimum required discount for subscription—which, in contrast, is homogeneous at 5-10% on the firm side of the market. We then confront respondents with a newsletter subscription vignette with a randomized level of nuisance and privacy in a two-by-two design. We find that a low level of privacy significantly raises the share of consumers who demand a higher-than-usual discount for subscription. However, neither privacy nor nuisance significantly affect the binary subscription decision. Zooming in on the privacy aspect to better understand the channels behind decisions in the vignette part, another survey element allowed participants to check the privacy rating associated with real-world newsletters through a fully functional tool. We solicited participants' reactions to the tool and recorded their level of interaction with it and uncovered substantial interest in the tool: Participants spent 83 seconds interacting with the tool on average, and 63% opted to analyze more newsletters than assigned to them in the task.

Our work relates to several strands of literature in economics, human-computer interaction, marketing, and privacy, which provides the behavioral background for the newsletter subscription scenario. For instance, Spiekermann et al. (2001) focus on the discrepancy between privacy intentions and actual behaviors. In an important contribution, Spiekermann et al. (2015) and Acquisti et al. (2016) provide an overview of the emerging markets for data and flag important privacy-related drawbacks of selling personal data online. In recent work in economics, Acemoglu et al. (2023) discuss the role of privacy guarantees in the market for data. Since email newsletters have (potentially hidden) privacy implications, we test how these difficulties in decision-making manifest in a frequent, familiar decision online. An important aspect related to the nuisance element of newsletters is cognitive load. Allcott et al. (2022) study the danger of digital addiction in relation to social media platforms, highlighting self-control problems of consumers when exposed to a constant stream of new information. We expect a similar pattern to apply in the context of high-frequency newsletters that cumulatively take up cognitive capacities and systematically exploit a consumer's fear of missing out (Dinh and Lee 2022; Neumann et al. 2023). Literature on marketing and consumer research reveals other potential dangers of newsletter nuisance, such as dangerous consumption addiction in online retail (Niedermoser et al. 2021; Rose and Dhandayudham 2014). Finally, Kumar (2021) shows the effect of newsletter design features on purchasing decisions that firms consciously use as a marketing tool.

We unify these diverse strands of literature by focusing on human-computer interaction in the context of

online retail newsletters. Our findings show heterogeneity in consumer reaction to newsletter features as well as choice patterns consistent with an intention-behavior gap and a high cognitive load that may make participants numb to relevant newsletter characteristics despite adjusting beliefs. In particular, the marked interest in privacy features of newsletters despite a lack of behavioral adjustment in reaction to low privacy calls for better, accessible, and interactive information for consumers.

## **Conceptual Background**

### ***Legal Background and Privacy Implications***

In recent years, many countries have introduced privacy regulations that address the usage of personal data by firms, with the European Union's General Data Protection Regulation (GDPR) being one of the most prominent ones. In Article 6, the GDPR only allows the processing of personal data if the data subject has given consent or if processing is necessary for the performance of a contract, for compliance with a legal obligation, for protecting the vital interests of the data subject, or for the purposes of public interest or legitimate interest. Article 4 further defines consent to be "any freely given, specific, informed and unambiguous indication of the data subject's wishes" and Article 7 requires firms to be able to demonstrate that data subjects have given consent and gives data subjects the right to withdraw consent at any time.

Kubíček et al. (2022) have analyzed the newsletter subscription forms of 1000 websites and successfully registered at 666 of them. They found that 17.3% of sites send emails without valid consent and 17.7% violate legal requirements by sending emails that lack content required by law. In total, they reported that 21.9% of websites were not compliant with regulations. Regarding the privacy implications of email newsletters, Englehardt et al. (2018) found that from a sample of 902 distinct senders, 30% leak the email address of the recipient to one or more third parties after opening the newsletter, implying a widespread prevalence of tracking in newsletter emails. Maass et al. (2019) developed a (now discontinued) web platform called PrivacyMail to automatically analyze newsletter emails. In a small-scale analysis of 20 services, they found that 80% of emails contained at least one resource hosted by a third party, with a maximum of 13 different third parties within a single email.

### ***Consumers and the Market for Email Newsletters—Theory***

This section describes the consumer's newsletter subscription decision. In this simple economic framework, preferences and beliefs guide the personal decision of whether or not to subscribe to an email newsletter. Specifically, newsletter subscription can be seen as the result of an expected utility maximization problem, where decision-makers trade off expected costs and benefits. The benefit side consists of the monetary benefits through newsletter-based direct discounts as well as the information value of the newsletter. The cost side of the utility maximization problem incorporates privacy and nuisance. With respect to privacy, rational decision-makers form beliefs about the amount and use of personal data that will be collected and stored by the firm. With respect to nuisance, beliefs about the frequency of unwanted or irrelevant newsletters allow decision-maker to determine expected costs of the mental and emotional effort of reading and managing future newsletters and their potentially undesirable consequences. Taking all this information into account, rational decision-makers set up their expected utility and maximize it by optimally choosing the number and type of newsletters to subscribe to. Naturally, when nuisance increases or privacy decreases, so does the cost of subscribing to the newsletter—which will in turn raise the minimum discount required by the consumer in order to subscribe. RQ1 and RQ2 address this standard economic mechanism by exploring baseline characteristics of the market for email newsletters as well as consumer reactions to varying levels of privacy and nuisance in the newsletter vignettes.

Based on the behavioral economics literature reviewed in the introduction, we investigate behavioral elements in subscription decisions in two ways: First, RQ3 explicitly evaluates interaction with and reaction to a newsletter privacy check. We capture consumers' willingness to obtain information as well as their reaction to the information (in terms of behavior as well as emotions and beliefs). Second, we use open questions to study participants' decision-making processes in both parts of the study. Thus, we explicitly allow and test for behavioral components of consumers' decision-making processes.

## Empirical Strategy

While the rational framework outlined in the previous section is straightforward, little is known empirically about how people form beliefs about privacy and nuisance costs of newsletters and trade these costs off against the monetary benefits. This section describes our survey design and sample used to shed light on consumer reactions to privacy-related and nuisance-related newsletter attributes.

### Survey Design

Due to the lack of prior empirical work, we first measure respondents' general newsletter-related attitudes and behaviors: To what extent do people subscribe to newsletters? Do they use tools to protect their privacy and manage their inbox? As a key quantitative measure, we elicit the self-reported real-life WTA for newsletter discounts (i.e., the self-reported minimum discount that, in a typical case, definitely induces a person to subscribe). These descriptives help us understand general newsletter strategies despite the casual nature of the subscription decision. They create a link between our experiment and real-world outcomes.

The figure shows two side-by-side survey forms for 'SLUSH - Freezing Cool Styles'. Both forms have the same header and main title: 'Sign Up for Our Newsletter and Get a 10% Discount!'. The left form (L) is titled 'Receive Monthly Updates on New Trends and Styles!' and includes a 'Gender' field with radio buttons for 'male', 'female', and 'diverse'. It has three required text input fields: 'First Name', 'Last Name', and 'Email Address\*'. Below the email field is a privacy statement: 'We will never share your email with anyone else.' and a checkbox 'Yes, I want to subscribe and receive 10% off my next purchase.\*'. The right form (R) is titled 'Receive Daily Updates on New Trends and Styles – You Won't Miss a Single New Item!'. It has a 'Gender\*' field with radio buttons for 'male', 'female', and 'diverse'. It has three required text input fields: 'First Name\*', 'Last Name\*', and 'Email Address\*'. Below the email field is a checkbox 'Yes, I want to subscribe and receive 10% off my next purchase.\*'. Both forms have a 'Submit' button at the bottom. The right form also includes a detailed Terms of Use and Privacy Policy statement below the checkbox.

**Figure 1. Two Vignettes. L: Low Nuisance & High Privacy; R: High Nuisance & Low Privacy.**

At the heart of the study, two survey elements confront respondents with 1) a newsletter vignette and 2) an interactive privacy tool. First, we run an experiment that assesses the nuisance and privacy beliefs surrounding the newsletter subscription decision: a vignette study where participants explore a newsletter subscription pop-up (including the privacy policy) for a hypothetical online fashion store. The experiment follows a 2x2 design with high / low nuisance and high / low privacy. The *low nuisance & high privacy* and *high nuisance & low privacy* vignettes are shown in Figure 1, intermediate cases are omitted from the figure. For nuisance, the vignette features vary in update rate (daily vs. monthly) and the note “You Won’t Miss a Single New Item!”. For privacy, the number of mandatory fields, the note “We will never share your email with anyone else”, and the information text on Terms of Use and Privacy Policy are altered. Clicking “Privacy Policy” opens a pop-up window with a privacy policy adapted from <https://www.privacypolicies.com/privacy-policy-generator/> and adjusted to the high / low privacy treatment.

Participants answer a set of questions about their emotional reaction to the vignette and their beliefs about nuisance and privacy levels of the newsletter. Assignment to the treatments is random, with group sizes of 148 (high nuisance x high privacy), 133 (h x l), 131 (l x h), and 119 (l x l). The randomization allows us to interpret differences in beliefs and choices between the four different groups causally.

Vignette studies are limited in scope due to their hypothetical nature. Thus, we bridge the gap between descriptive real-world evidence and causal hypothetical-scenario evidence through our second survey element. Here, we only focus on privacy aspects. This part of the study uses real-world newsletters and an authentic tool that allows participants to analyze these newsletters with respect to privacy. We offer a small portfolio of seven German online retail newsletters that score differently with respect to privacy. We ask participants to analyze one of these newsletters by using a self-programmed tool that provides a realistic expert assessment of privacy-relevant newsletter aspects. The assessments and the information shown by the tool are based on the discontinued website PrivacyMail.info (Maass et al. 2019).

Some participants are allowed to select into analyzing a newsletter they are actually subscribed to (a more natural setting) while others are randomly assigned a newsletter to analyze (a cleaner design without selection effects). As the core set of outcomes, we track their interaction with the tool as a measure of effort and interest.<sup>1</sup> To connect the two main parts of the survey, we ask all participants about their reaction to the result of the privacy check and their minimum willingness to accept the newsletter (measure see above). We finally offer participants easy access to the newsletters presented in the study as well as access to general resources about unsubscribing from newsletters and track their interest in both types of information.

In addition to the quantitative WTA items and standard Likert scales to capture beliefs, we also use open questions to elicit participants' reactions to the vignette and privacy tool. Responses for the tool reaction were coded by one of the authors and validated for a 10% subsample by an external research assistant with Cohen's Kappa between 0.57 and 1.00 (mean: 0.73) for the tool.

### ***Sample and Ethical Aspects***

The study was conducted in 2022 with participants recruited from university students in two large business administration and information systems courses. In total, 527 students participated in the survey. 57% of participants identified as male, 41% as female, 0.2% as diverse or non-binary, and 2% preferred not to answer. The majority of participants were management students (74%). The remainder of participants were students of information systems (17%), computer science (7%), and other fields (2%). Prior to collecting survey data, we obtained IRB approval from the Ethics Committee of the Catholic University of Eichstaett-Ingolstadt for the survey design and procedures. Participation in the study was voluntary. Student participants were rewarded for their participation with a bonus code that could be redeemed as part of a series of grade bonus tasks in their university course. This code was not stored with the collected data. The only condition for receiving the reward was completion of the survey.

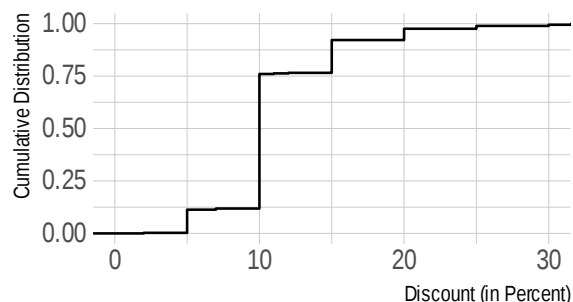
## **Main Results**

### ***The Newsletter Subscription Market***

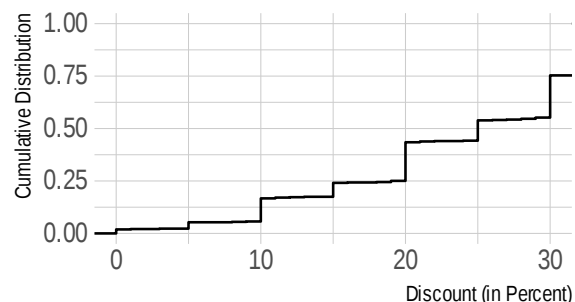
To answer RQ1, this section describes the market for online newsletter subscriptions in general before subsequent sections zoom in on specific facets. An interesting feature of the newsletter subscription decision in contrast to other privacy-related online decisions (i.e., creating a social media account) is the simple market involved in the decision: Online retailers typically offer specific discounts in exchange for a newsletter subscription that consumers can then accept or decline. Figure 2 shows the distribution of discount offers for 2,099 firms that are active in Germany in 2020, based on a German coupon comparison site. Most firms offer a discount in the 5 to 10% range or an absolute equivalent to that with a 5 to 10 Euro discount relative to a minimum order value of 50 Euros. Thus, willingness-to-pay for a newsletter subscription is quite homogeneous on the firm side—suggesting that this market has converged to an equilibrium.

---

<sup>1</sup>We also elicit privacy-related attitudes based on the informational privacy and psychological privacy scales by Dienlin and Trepte (2015), which remained unaffected by the interaction with the privacy tool.



**Figure 2. Discounts Offered by Firms for Newsletter Subscription.**



**Figure 3. Minimum Discount Users are Willing to Accept for Subscription.**

On the supply side of the market for data, Figure 3 plots the (categorized) minimum accepted discounts. The figure reveals that our participants tend to demand quite high minimum discounts, with only approximately 20% of participants accepting the 5 or 10% discounts that are standard in the newsletter market and would be expected to be market-clearing.<sup>2</sup> How do these general WTAs manifest as real-world newsletter subscription choices made by the respondents? With respect to general subscription behavior, there is significant heterogeneity within the sample. 18% of participants are not currently subscribed to any email newsletters. These participants also indicated a slightly higher minimum discount (2 percentage points higher) that would induce them to subscribe—indicating that their stated preferences and personal choices align. On average, participants are subscribed to 7.4 newsletters, with women being subscribed to significantly more newsletters (9.4 on average) than male and non-binary participants (6.0 on average).

Besides general subscription behavior, consumers have several additional tools available to manage their newsletters with respect to both nuisance and privacy. One prominent strategy is to subscribe to the newsletter to benefit from the immediate discount but then to unsubscribe again. 84% of participants report using this strategy. Of those participants who subscribe to unsubscribe, 88% admit that they will *forget* to unsubscribe at times. Unintentionally staying subscribed would imply that the consumers are facing privacy costs without reaping any long-term rewards. Another important strategy is inbox management, e.g., a separate email address or using email inbox filters. More than half of participants (58%) use at least one inbox management strategy. 34% of participants use a designated email address and 35% use email filters.

Overall, this descriptive analysis of the market for data reveals substantial heterogeneity in consumer preferences regarding subscription as well as their willingness to accept discounts. On the firm side, however, discount offers are surprisingly homogeneous. The subsequent sections will focus on the consumer side of the market and zoom in on specific components of the newsletter subscription decision.

### ***The Effect of Newsletter Characteristics on Subscription and Beliefs***

In order to answer RQ2, we confronted participants with one of four newsletter subscription forms featuring variations in nuisance and privacy. After interacting with the respective subscription form, we asked participants for their willingness to subscribe to the hypothetical newsletter. 67% of participants indicated that they would not be willing to subscribe to the newsletter. As shown in column (1) of Table 1, nuisance and privacy have no significant effect on the subscription decision. Describing reasons behind their subscription decision (see Figure 4), participants clearly focus on the discount, but some prominent mentions also relate to privacy (“spam”, “data”) and nuisance (“daily”).

Only 4% of participants would regularly open and read the SLUSH newsletter when subscribed. As for the subscription decision, we find no significant effect of nuisance or privacy on the likeliness of reading the newsletter (column (2) of Table 1). Explanatory power of the regression is low, which is likely due to the overall complexity of newsletter preferences (see previous sections). Asked whether they expect to receive

<sup>2</sup>One reason for these high demands arguably lies in the abstract nature of the question, where we ask about their preferences regarding a *typical* newsletter. The experimental sections of this paper will explore more specific and applied newsletter subscription decisions.

**Table 1. Regression Results for Newsletter Subscription and Expectations.**

	<i>Dependent variable:</i>			
	Subscription <i>ordered log.</i>	Open & Read <i>ordered log.</i>	3rd-Party Spam <i>ordered log.</i>	WTA Increase <i>logistic</i>
	(1)	(2)	(3)	(4)
High Nuisance	-0.051 (0.156)	-0.166 (0.174)	0.340** (0.155)	0.198 (0.214)
Low Privacy	0.071 (0.156)	-0.161 (0.174)	0.650*** (0.156)	0.510** (0.214)
Female	0.561*** (0.159)	0.336* (0.175)	0.209 (0.157)	0.287 (0.214)
Shopping Freq.	-0.189*** (0.063)	-0.234*** (0.073)	0.167** (0.065)	-0.093 (0.087)
Observations	527	527	527	527
Pseudo R <sup>2</sup>	0.013	0.014	0.015	0.018

*Notes.* The table reports the effects of nuisance and privacy on subscription behavior and expectations. Standard errors are in parentheses below the estimates. (1) to (3) are measured on 7-point Likert scales. WTA Increase (4) describes whether participants have a higher WTA for subscribing to the hypothetical newsletter than for subscribing to newsletters in general. \*p<0.1; \*\*p<0.05; \*\*\*p<0.01

spam from third parties after subscribing, 61% think that it is likely that they would not only receive the newsletter but also unwanted emails from other parties. Here, we find a significant effect of both nuisance and privacy on the perceived likelihood of third-party spam (column (3) of Table 1). This is also reflected in the descriptive numbers. For the “best-case” newsletter (low nuisance, high privacy), 49% of participants expect to receive third-party spam while, for the “worst-case” newsletter (high nuisance, low privacy), 73% expect third-party spam.

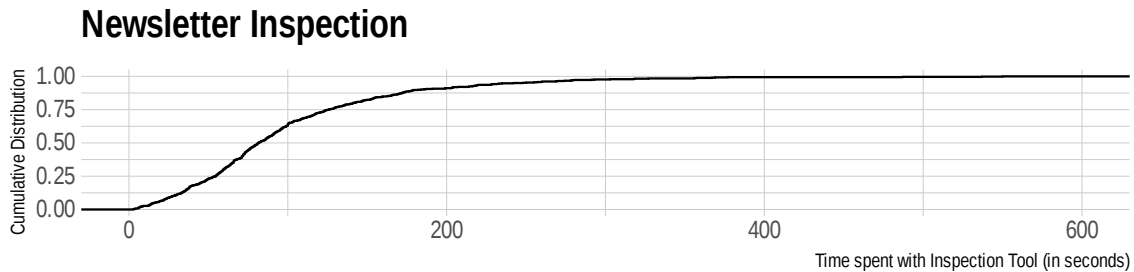
**Figure 4. Reactions to Subscr. Form.****Figure 5. Reactions to Privacy Check.**

Furthermore, we asked participants if they would subscribe to the newsletter for receiving a discount coupon and, if yes, how high the discount would have to be. This question was analogous to the general question shown in the first part of the survey, which is described in a previous section. We tested for differences in the willingness to accept a coupon code for subscribing between the general newsletter and the SLUSH newsletter. With a median of 20% for both the general and the SLUSH newsletter (means: 20.2% and 20.0%), users show similar expectations regarding the value of the discount code for both cases. However, for 22% of participants there is an increase of WTA from the general case to the SLUSH newsletter. Analyzing this WTA increase, we find that being confronted with a low-privacy newsletter subscription form significantly

increases the likelihood that users demand a higher discount value. The results of the logistic regression are shown in column (4) of Table 1.

### Consumer Reaction to an Interactive Newsletter Privacy Check

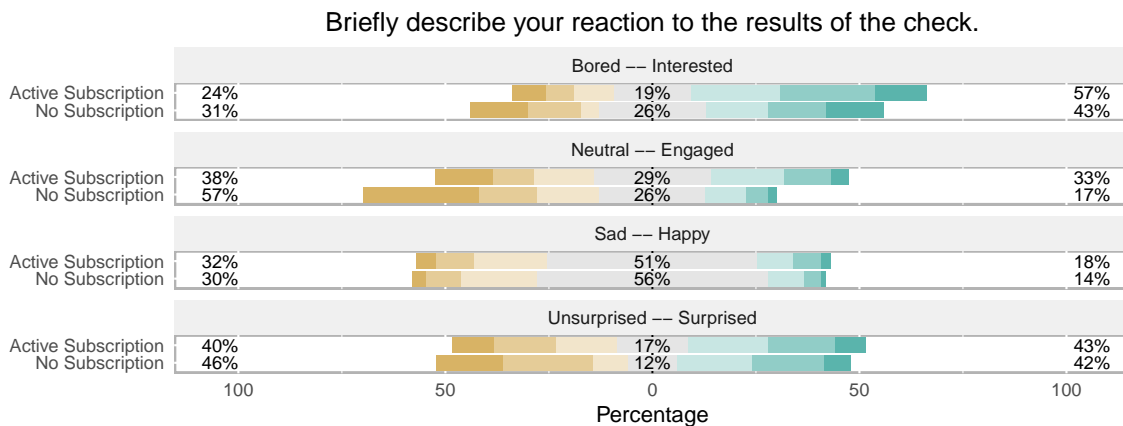
In the final part of the survey, we confronted participants with an interactive tool to learn about the privacy characteristics of different newsletters. To answer RQ3, we measured how they interacted with and reacted to this tool. 171 participants (32%) were active subscribers to at least one of the seven newsletters. These participants were randomly assigned to one of the newsletters with an active subscription. The other 356 participants were randomly assigned to one of the seven newsletters.



**Figure 6. Time Participants Spent with Newsletter Inspection Tool.**

440 participants (83%) used the tool to analyze at least one of the provided newsletters. The median time spent using the tool was 83 seconds (first quartile: 55 seconds, third quartile: 129.5 seconds). Figure 6 shows the cumulative distribution of interaction times.

Participants analyzed 3.8 newsletters on average (median: 3.0). Only 17% analyzed no newsletters, while 36% analyzed all 7 newsletters. After analyzing newsletters, participants were shown the privacy rating and additional information on the factors that influenced this rating: The numbers of contacted companies, the prevalence of personalized links, and whether cookies are set. Participants could then also click to receive more details on contacted companies (64%), personalized links (50%), and cookies (46%).



**Figure 7. Reactions to Privacy Check.**

When asked on the privacy rating of their assigned newsletter, 55% of participants were able to remember this rating after using the tool. 43% of participants with an active subscription to one of the newsletters intended to unsubscribe after seeing the results of the check. In general, participants displayed interest in using a privacy analysis tool for their newsletter emails. When describing their reaction to the check in their own words (see Figure 5), participants focus on the element of surprise (or lack thereof) and on the “companies” involved. In their free-text answers, 9.2% of participants made explicit remarks regarding the privacy practices of newsletter issuers. 39% of them think that the current privacy practices should be



changed (e.g., “I don’t think that forwarding your customers’ information to third parties without very clearly stating this should be legal.”) while 61% don’t expect a change (e.g., “I feel like it’s safe enough to use the website.”).

Figure 7 gives an overview of the reactions to the check results, measured on 7-point emotion scales. 54% of participants were interested in the results of the check, while 26% were bored. We distinguish participants who indicated to be registered to one or more newsletters in real life from those with no active newsletter subscriptions at all. For interest ( $p = 0.029$ ) and engagement ( $p < 0.001$ ), we find significantly higher values in the active subscription group. For the other attributes, there are no significant differences ( $p > 0.2$ ).

## Discussion and Concluding Remarks

1,000 unread emails in your inbox and 900 of them are e-mail newsletters from that one shop you had signed up for back in the day to take advantage of the 10% discount—a scenario that may sound familiar to many readers in the age of online shopping. In this paper, we take a closer look at the newsletter subscription decision and document consumers’ reluctance to adjust their actual (binary) subscription decision based on nuisance and privacy as newsletter characteristics, although they are adjusting their beliefs about consequences of subscription. In the privacy domain, this reluctance is consistent with the discrepancy between privacy intentions and actual behavior described in Spiekermann et al. (2001). In relation to nuisance, consumers may have been numb to email newsletter features—other than the discount—due to overexposure over time, which leaves us with a very small group of potential compliers. This may have been exacerbated by the drawback that it was likely difficult for participants to treat the hypothetical subscription form as if it were real. Thus, the external validity of these findings is limited by the task as well as the student sample. For the subgroup of those who would, in principle, subscribe ex-ante, the behavior would also be consistent with present bias or digital addiction or fear of missing out (Allcott et al. 2022; Neumann et al. 2023). Future research should focus on these factors as well as on the specific role of cognitive load.

At the same time, we find a significant and positive effect of low newsletter privacy on consumers’ expectation of receiving third-party spam and the share of customers who require a higher-than-usual discount for subscription. Especially the remarkable effect on spam beliefs, with a difference of 24 percentage points between high and low privacy groups, shows that users indeed understand the fine print of subscription forms. Together with the substantial interest participants show in the privacy tool and their emotional reactions, these findings connect to insights from the privacy policy literature. In the context of privacy policies, users are being confronted with policies of increasing length (Linden et al. 2020) which makes it more and more difficult to fully process and understand their contents and further contributes to the overload discussed above. Visual enhancements can significantly improve user experience and comprehension of policies and textured agreements (Kay and Terry 2010; Reinhardt et al. 2021; Tabassum et al. 2018). The high interaction rates and interest we find in this study’s privacy tool imply an analogous effect on newsletter subscription forms. To consumers, privacy is not a mere side note. They are willing and able to understand the privacy implications and take them into account in their subscription decision if they receive proper and accessible information. Since culture affects both privacy attitudes (Li et al. 2017) and life-long learning (Hartinger 2023), further research should examine its role in online behavior to optimize such policies in the context of new technologies and phenomena, such as email newsletters. Overall, there is ample scope for future research to exploit the simple market structure of the market for email newsletters to study digital addiction, information overload, and privacy. The intention-behavior gap in our findings, despite emotional and intellectual involvement, only underlines the importance of the seemingly casual subscription decision.

## Acknowledgements

We would like to thank the participants of our study for contributing their time, Simon Wiederhold, Fabian Mierisch, and the anonymous reviewers for their helpful feedback, and Chantal Endlicher for her valuable research assistance. We further are grateful for funding support from the Bavarian Research Institute for Digital Transformation (bidt). Responsibility for the contents of this publication rests with the authors.

## References

- Acemoglu, D., Fallah, A., Makhdoumi, A., Malekian, A., and Ozdaglar, A. 2023. *How Good Are Privacy Guarantees? Platform Architecture and Violation of User Privacy*. Working Paper 31413. National Bureau of Economic Research, 2023.
- Acquisti, A., Taylor, C., and Wagman, L. 2016. “The Economics of Privacy,” *Journal of Economic Literature* (54:2) 2016, pp. 442–492.
- Allcott, H., Gentzkow, M., and Song, L. 2022. “Digital Addiction,” *American Economic Review* (112:7), pp. 2424–2463.
- Cases, A.-S., Fournier, C., Dubois, P.-L., and Tanner, J. F. 2010. “Web site spill over to email campaigns: The role of privacy, trust and shoppers’ attitudes,” *Journal of Business Research* (63:9), pp. 993–999.
- Dienlin, T. and Trepte, S. 2015. “Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors,” *European Journal of Social Psychology* (45:3), pp. 285–297.
- Dinh, T. C. T. and Lee, Y. 2022. ““I want to be as trendy as influencers” – How “fear of missing out” leads to buying intention for products endorsed by social media influencers,” *Journal of Research in Interactive Marketing* (16:3), pp. 346–364.
- Englehardt, S., Han, J., and Narayanan, A. 2018. “I never signed up for this! Privacy implications of email tracking,” *Proceedings on Privacy Enhancing Technologies* (2018:1) 2018, pp. 109–126.
- Hartinger, K. 2023. *Individualism, Creativity, and Innovation*. Discussion Paper 2313. IPP.
- Kalantari, S., Put, A., and De Decker, B. 2021. “Trackers in Your Inbox: Criticizing Current Email Tracking Practices,” in: *Privacy Technologies and Policy: 9th Annual Privacy Forum, APF 2021, Oslo, Norway, June 17–18, 2021, Proceedings*, Berlin, Heidelberg: Springer-Verlag, pp. 156–167.
- Kay, M. and Terry, M. 2010. “Textured agreements: Re-envisioning electronic consent,” in: *Proceedings of the Sixth Symposium on Usable Privacy and Security, SOUPS ’10*. New York, NY, USA: Association for Computing Machinery, pp. 1–13.
- Kubiček, K., Merane, J., Cotrini, C., Stremitzer, A., Bechtold, S., and Basin, D. 2022. “Checking Websites’ GDPR Consent Compliance for Marketing Emails,” *Proceedings on Privacy Enhancing Technologies* (2022:2) 2022, pp. 282–303.
- Kumar, A. 2021. “An empirical examination of the effects of design elements of email newsletters on consumers’ email responses and their purchase,” *Journal of Retailing and Consumer Services* (58). Article 102349.
- Li, Y., Kobsa, A., Knijnenburg, B. P., and Carolyn Nguyen, M.-H. 2017. “Cross-Cultural Privacy Prediction,” *Proceedings on Privacy Enhancing Technologies* (2017:2) 2017, pp. 113–132.
- Linden, T., Khandelwal, R., Harkous, H., and Fawaz, K. 2020. “The Privacy Policy Landscape After the GDPR,” *Proceedings on Privacy Enhancing Technologies* (2020:1), pp. 47–64.
- Maass, M., Schwär, S., and Hollick, M. 2019. “Towards Transparency in Email Tracking,” in: *Privacy Technologies and Policy*, M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina, and A. Bourka (eds.). Lecture Notes in Computer Science. Cham: Springer International Publishing, pp. 18–27.
- Neumann, D., Huddleston, P. T., and Behe, B. K. 2023. “Fear of Missing Out as motivation to process information: How differences in Instagram use affect attitude formation online,” *New Media & Society* (25:1), pp. 220–242.
- Niedermoser, D. W. et al. 2021. “Shopping addiction: A brief review.” *Practice Innovations* (6:3), pp. 199–207.
- Reinhardt, D., Borchard, J., and Hurtienne, J. 2021. “Visual Interactive Privacy Policy: The Better Choice?,” in: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI ’21*. New York, NY, USA: Association for Computing Machinery, pp. 1–12.
- Rose, S. and Dhandayudham, A. 2014. “Towards an understanding of Internet-based problem shopping behaviour: The concept of online shopping addiction and its proposed predictors,” *Journal of Behavioral Addictions* (3:2), pp. 83–89.
- Spiekermann, S., Acquisti, A., Böhme, R., and Hui, K.-L. 2015. “The challenges of personal data markets and privacy,” *Electronic Markets* (25:2), pp. 161–167.
- Spiekermann, S., Grossklags, J., and Berendt, B. 2001. “E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior,” in: *Proceedings of the 3rd ACM Conference on Electronic Commerce, EC ’01*. Tampa, Florida, USA: Association for Computing Machinery, pp. 38–47.

- Tabassum, M., Alqhatani, A., Aldossari, M., and Richter Lipford, H. 2018. "Increasing User Attention with a Comic-based Policy," in: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18. New York, NY, USA: Association for Computing Machinery, pp. 1–6.
- White, T. B., Zahay, D. L., Thorbjørnsen, H., and Shavitt, S. 2008. "Getting too personal: Reactance to highly personalized email solicitations," *Marketing Letters* (19:1) 2008, pp. 39–50.