Right Here, Right Now: User Perceptions of In-Place Contextual Privacy Options

Florian Dehling
Justus Liebig University Giessen
Giessen, Germany
florian.dehling@uni-giessen.de

Jan Tolsdorf
The George Washington University
Washington, D.C., USA
jan.tolsdorf@gwu.edu

Luigi Lo Iacono
Justus Liebig University Giessen
Giessen, Germany
luigi.lo_iacono@uni-giessen.de

***Abstract*—In modern online services and apps, legally required privacy information and controls are often placed on separate pages or menus, forcing users to leave their primary tasks to review privacy statements or adjust settings. This disrupts usability by causing unnecessary friction, context switching, and information overload. We propose In-Place Contextual Privacy Options (IPCPOs), a Transparency-Enhancing Technology (TET) that integrates relevant privacy controls directly into a user's workflow. IPCPOs tailor privacy information and settings to the immediate context, reducing the set of controls and information provided to contextual needs. In a study with 442 participants in an e-commerce setting, we found that IPCPOs should prioritize information on personal data types, processing purposes, and data recipients, alongside offering privacy controls. While IPCPOs score high on perceived transparency, only perceived control and privacy concerns significantly drive adoption intention. This work demonstrates how IPCPOs help comply with data protection obligations while reducing usability burdens.**

***Index Terms*—transparency-enhancing technology, tet, contextual transparency, contextual privacy control, sem**

1. Introduction

Modern online services inherently rely on personal data processing, such as handling orders in e-commerce, enabling media sharing on social platforms, or making personalized content recommendations on streaming services. Data protection laws, such as the European General Data Protection Regulation (GDPR), require online service providers processing personal data to offer data subjects clear, comprehensive information and control over how their data are handled. Such privacy-related transparency and control mechanisms are typically provided through separate privacy settings pages and privacy statements. These settings and statements summarize all available privacy options and outline ongoing data processing activities. However, if users wish to check or adjust how their personal data is handled while placing an order, sharing media, or consuming content, they must leave their current task to navigate privacy menus or read lengthy privacy statements.

This state of the art has two major issues: (1) Privacy statements are often lengthy and filled with legal jargon, making them cumbersome to read and difficult to understand. Studies show that traditional textual policies fail to effectively inform users about data handling, for example, because variations in wording lead to inconsistent interpretations, with even experts struggling to agree on their meaning [1], [2]. (2) Forcing users to exit their current task (e.g., interrupting checkout to review privacy policies or update settings) introduces significant usability friction [3], increasing the risk of neglecting privacy settings and remaining unaware of their actions' consequences.

We argue that an effective human-centered privacy design should minimize disruption by embedding context-relevant privacy controls into a user's workflow, reducing friction while maintaining transparency and control options. For this purpose, we propose In-Place Contextual Privacy Options (IPCPOs), a Transparency Enhancing Technology (TET) that reduces the amount of relevant information and privacy settings through a visually interactive user interface embedded into the current usage context. The idea of IPCPOs is informed by previous user-centered research, finding that enhanced visual presentations like privacy labels or tabular formats make privacy statements more accessible [4]–[6], while tailoring privacy statements to specific usage contexts reduces the amount of relevant information, thereby shortening the texts users need to read [7], [8]. IPCPOs combine these findings and extend their application to contextually fitting privacy settings. As a result, only a minimal context switch, i.e., triggering an overlay, is required to retrieve privacy-related information and make informed decisions on the processing of their personal data.

In this paper, we present a prototype implementation of IPCPOs in the context of an e-commerce platform and evaluate user perceptions toward IPCPOs by conducting an online user study with 442 participants. Using a between-subject design, we compared three different implementation approaches of IPCPOs to identify the version participants were most satisfied with in terms of perceived transparency and perceived control, as well as their intention to make use of IPCPOs if they were available in practice. To this end, we answer the following research questions:

(RQ1) Which legally required information should IPCPOs prioritize to balance regulatory obligations with conciseness and perceived usefulness? We find that e-commerce users prioritize information on the type of personal data processed, processing purposes, and data recipients. Additional legally required information on whether personal data are processed outside the EU or are used for profiling was considered less important. When comparing IPCPOs that focus on either the type of personal data or the purpose of processing and hide the remaining aspects in second-layer menus in the UI, we do not identify any user preference. This highlights the need for IPCPOs to focus on either of these key aspects when designing interfaces that balance conciseness with user information needs.

(RQ2) How do interactive elements and control features in IPCPOs impact users' perceived privacy control and information efficacy compared to text-based IPCPOs? When comparing a purely text-based IPCPO with interactive IPCPOs that also offer control settings, users clearly preferred the latter. Participants showed a significantly higher intention to adopt interactive IPCPOs and felt they provided greater control over their privacy choices, but not more transparency. Even simple text-based IPCPOs are thus useful in improving transparency toward users.

(RQ3) How do perceived control, perceived transparency, and privacy concerns influence users' intention to adopt IPCPOs? The perceived level of control over personal

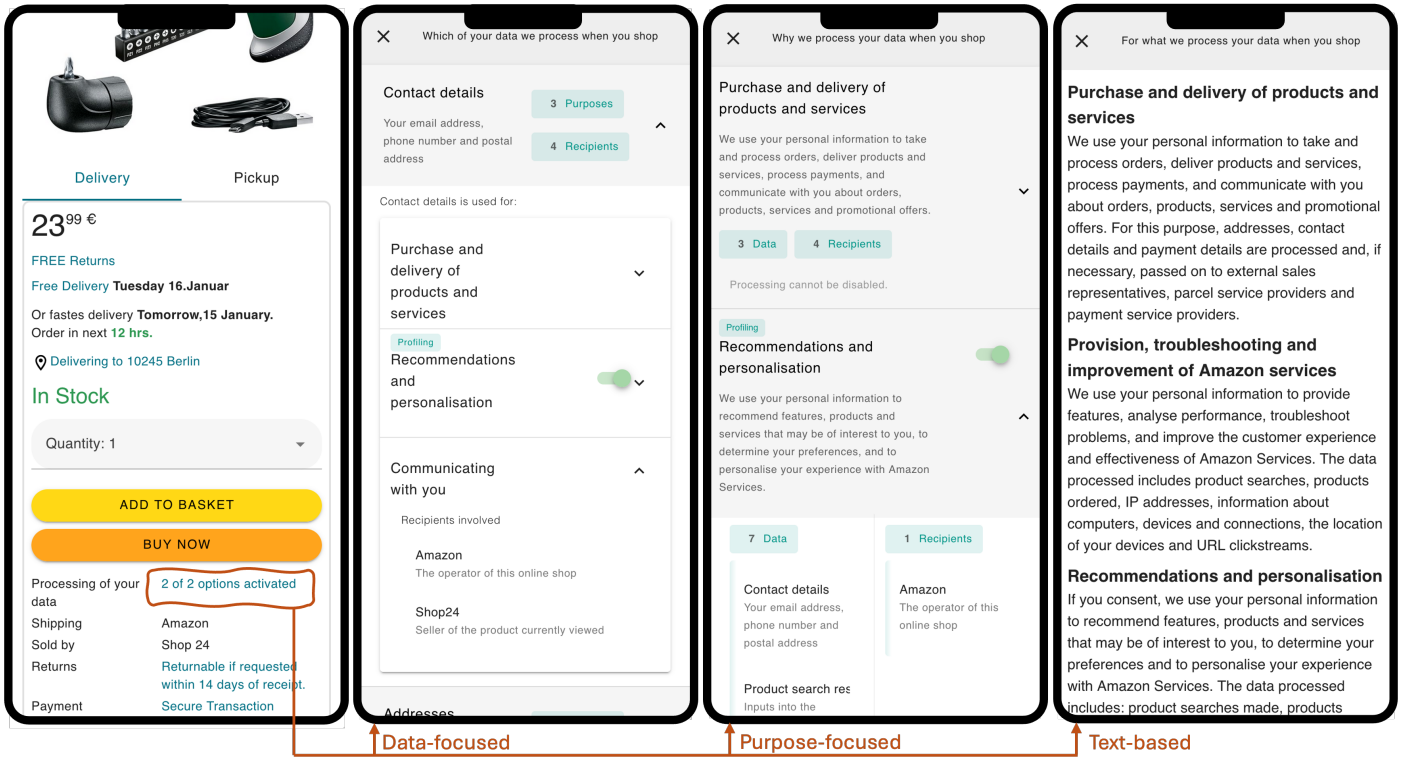

Figure 1: Screenshots from the prototype as been used in the study. The left picture shows the integration of the IPCPO in a product view of the Amazon webshop. After tapping on the link, the IPCPO opens. The other pictures show each of the IPCPO variants with all layers expanded for an exemplary data category or purpose.

data processing provided by IPCPOs was the strongest predictor of users' intention to adopt IPCPOs. While perceived transparency offered by IPCPOs and participants' privacy concerns were also significant, they had considerably smaller effects.

Our work contributes to the practical implementation of data subject rights by demonstrating how IPCPOs can balance regulatory compliance and usability aspects. We provide the necessary empirical insights to inform the design of context-aware, user-centric privacy interfaces, offering a scalable approach to improving privacy interactions in online services.

2. Background

This section provides foundations on legal obligations concerning transparency and control set by the GDPR, related work on advanced visual presentation of privacy information and controls, and the contextual tailoring and presentation of privacy details.

2.1. Legal Obligations on Providing Control and Transparency to Data Subjects

Entities that process personal data in the European Union (EU) or handle data of individuals residing in the EU (i.e., data subjects) are subject to the General Data Protection Regulation (GDPR). Among other provisions, the GDPR mandates extensive transparency and control mechanisms for data subjects. Specifically, Article 13 establishes the legal obligation to provide data subjects with clear and comprehensive information at the time their personal data is collected. This includes details about the data controller and any recipients of the personal data, the purposes and legal basis for processing, the duration for which data will be stored, and information on data subjects' rights. These rights extend beyond transparency—such as access to personal data (Articles 15 & 20)—to active intervention, including the right to rectify or erase data (Articles 16 & 17), restrict or object to processing (Articles 18 & 21), and object to automated decision-making (Article 22). Additionally, data subjects have the right to withdraw previously given consent at any time (Article 7), with consent required to be freely given, specific, informed, and unambiguous.

The GDPR does not specify how these rights and information obligations must be implemented, apart from any information being in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12). However, in practice, data controllers have largely relied on lengthy, text-heavy, legalese-laden privacy statements, which have become the de facto standard [9]. These documents consolidate all legally required information in a single location and are usually only actively shown to users when they register for an online service for the first time. Meanwhile, privacy statements have been widely criticized for being ineffective and difficult for users to understand [1], [2]. Corresponding intervention mechanisms are implemented in various locations, such as account settings or dedicated websites accessible via links within privacy statements [10].

2.2. Related Work

To address the limitations associated with lengthy, text-based, legalese-laden privacy policies, research has suggested a variety of strategies aimed at enhancing the usability of communications concerning data protection-related information. One focus is on structuring and visualizing information. Bahrini, Zargham, Wolff, *et al.* [11] developed a one-pager text-based privacy policy optimized for smartphone displays. Their evaluation has shown that, in particular, a clearly structured presentation of the text components helps users grasp information and thus leads to a low workload when obtaining data protection information. Kelley, Bresee, Cranor, *et al.* [6] have developed a standardized structure for the contents of data protection declarations and used it to implement both text-based short privacy policies and tabular presentations, also known as Privacy Policy Nutrition Labels. A study has shown

that standardized structure leads to an improved understanding among readers, while the form of presentation (text-based or tabular) is less critical [12]. Reinhardt, Borchard, and Hurtienne [5] redesigned the Privacy Policy Nutrition Label table by adding visual interactive components that provide further information and controls. Their evaluation revealed that the interactive features attract users' attention and thus encourage them to examine data protection aspects more closely. Zhang, Klucinec, Norton, *et al.* [4] applied the concept of Privacy Nutrition Labels on iOS privacy labels using an expandable grid layout. Using a prototype in a user study, participants were able to answer content-related questions faster and with fewer errors than with the original iOS privacy labels.

To address the limitations of traditional privacy policies, another approach is to structure and contextualize them, providing only the relevant information based on a user's activity [13]. Ortloff, Windl, Schwind, *et al.* [8] developed a browser plugin for desktop computers that embeds contextual privacy policies directly into websites, displaying relevant information about data collection and processing purposes based on a user's current activity, such as searching for or purchasing a product on an e-commerce platform. Their evaluation with 15 participants showed a general preference for the concise texts presented. However, qualitative feedback highlighted limitations, including habituation effects caused by repeated exposure and the need for visual elements rather than plain text to improve user engagement and avoid information overload.

Contributions. To the best of our knowledge, our study on In-Place Contextual Privacy Options (IPCPOs) is the first to investigate user perceptions of contextually relevant transparency and control mechanisms inbuilt into the primary task, empirically investigating their effectiveness with 442 participants. Unlike prior approaches, we propose a design that seamlessly integrates privacy options into a user's workflow on desktop and mobile environments while empirically assessing which privacy information users find most relevant. This approach minimizes information overload and avoids disruptions to the primary task. Additionally, our study offers the first empirical insights into the key factors that motivate users to engage with contextual transparency and control mechanisms.

3. In-Place Contextual Privacy Options

In-Place Contextual Privacy Options (IPCPOs) build on prior research by combining visualized presentation with context-aware content adaptation, ensuring that privacy information and controls to provide and to withdraw consent are seamlessly integrated into users' primary tasks. This integration reduces friction, enhances usability, and strengthens user autonomy over personal data decisions. In the following, we outline the design requirements for IPCPO and present their prototype implementation.

3.1. Design Requirements

The IPCPO concept is designed to deliver relevant privacy information and controls to users as they interact with an online service without requiring them to leave their primary usage context completely. This goal results in four essential requirements:

Seamless Integration. IPCPOs should integrate into the primary user interface without causing disruption [14]. Hence, the primary user interface should undergo minimal changes. Users must be able to access IPCPOs without altering their current context, such as navigating to a different URL.

Filtering of Information. IPCPOs should display information relevant to the current user action [13]. Instead of presenting an exhaustive list of data processing—as central privacy policies do—IPCPOs filter content to align with the specific application context. This approach reduces the volume of information and offers more specific details.

Information Compression. IPCPOs must compress information to facilitate user comprehension with minimal cognitive effort [8]. While tailoring content to the current usage context, it may still be necessary to present information on a variety of data processing. To ensure users access these details with minimal cognitive load, the information should be structured and prioritized to allow users to effectively engage with privacy information and controls during their primary interaction.

Control mechanisms. IPCPOs should provide not only transparency information but also control functions that allow users to consent to or withdraw from data processing [5]. Unlike the current standard, which typically centralizes controls in specific settings, IPCPOs make these controls readily accessible within the current context of use. This approach eliminates the need for users to change contexts and disrupt their primary tasks. Additionally, it clearly delineates which data processing activities related to a specific task users can actually control, since, in practice, controls are usually offered only for data processing conducted on the legal basis of consent.

3.2. Study Prototypes

We developed three web-based high-fidelity prototypes [15] to explore the effectiveness of In-Place Contextual Privacy Options (IPCPOs) (cf. Fig. 1). We chose Amazon's e-commerce platform as the application context for our prototypes. This decision was based on several key factors: Amazon offers a wide range of services that process personal data, including voice assistants, audio and video content streaming, and using Amazon's e-commerce platform to sell goods as a merchant. Consequently, the central privacy statement available on the website includes information, e.g., processed data categories, that cover all possible services offered, while for purchasing goods in the webshop, only a fraction of information is actually relevant. Furthermore, since third-party sellers can use Amazon's e-commerce platform to offer their goods, the recipients of data may vary between products. This variability is challenging to convey through central privacy statements. However, IPCPOs address this by providing context-specific filtering and presentation of information. Finally, Amazon's extensive user base increases the likelihood that our study participants are familiar with the platform from prior experience.

For the specific use case, we selected Amazon's product selection process, where users decide to purchase a specific product. A text link below the "Buy Now" button (cf. Fig. 1) opens an IPCPO view as an overlay, eliminating the need to leave the current user context completely. The overlays are displayed in full-screen on smartphones and partial-screen on desktops. The link text indicates the number of optional data processing operations currently enabled, specifically those requiring user consent under Art. 6 (1) lit. a of the GDPR. We opted not to use an icon, as research suggests that icons can be misleading, whereas link text offers clearer communication [16].

In total, we prototyped three variations of IPCPO views, each differing in transparency, control, and information prioritization. Each prototype variation presents privacy information differently. However, all versions consistently provide the same information about processing purposes, data processing cate-

gories, recipients involved, options to prevent data processing, and details about profiling and data processing outside the EU.

Data-Focused Prototype. The data-focused IPCPO prototype presents an overview of data categories, providing examples of specific data within each category. It also indicates the number of purposes that utilize each data category and the number of data recipients involved. Users can expand a data category to view a list of purposes for which the data are used. Labels identify purposes that involve profiling or processing outside the EU, and a toggle switch allows users to enable or disable optional data processing. Additionally, users can expand a processing purpose to examine detailed information about the data recipients involved (cf. Fig. 1, *Data-focused*).

Purpose-Focused Prototype. The purpose-based IPCPO prototype provides an overview of processing purposes, each accompanied by a brief explanatory text. Users can activate or deactivate optional processing purposes using a toggle switch. Each purpose also displays the number of data categories processed and the number of recipients involved. By expanding a purpose, users can view detailed information, including the processed data, involved recipients, and examples or brief explanations (cf. Fig. 1, *Purpose-focused*).

Text-Based Prototype. The text-based IPCPO prototype features a paragraph for each processing purpose, briefly explaining it. It lists the processed data categories and the involved recipients. The text also indicates whether a processing purpose requires consent or involves profiling or data processing outside the EU. Unlike the data- and purpose-focused variations, the text-based version does not offer a direct option to enable or disable data processing (cf. Fig. 1, *Text-based*).

4. Quantitative Evaluation

To evaluate our prototyped IPCPOs, we conducted an online user study with 442 participants from Germany, employing a between-subject design. In the following, we provide an overview of the measurement instruments used for the evaluation and the experimental procedure.

4.1. Ethical Considerations

Although our institution does not have a formal IRB, we took steps to minimize potential harm to our participants. This study adhered to rigorous ethical standards of the German Research Foundation, and we ensured that all participants provided informed consent before starting the survey. The study procedure was reviewed and approved by the data protection officer at our institution. Participants were recruited through the online panel Prolific and received €1.57 for their participation, which corresponds to an hourly rate of approximately €14.85 based on an average completion time of six minutes. To safeguard participants' confidentiality, all data was collected under pseudonyms provided by Prolific. The research data collected is stored in our organization's research data management system in accordance with the strict requirements of the German Research Foundation.

4.2. Research Design

Perceived Relevance of Data Processing Information. As discussed in Sec. 2.1, the GDPR mandates that data subjects be informed about personal data processing, including processing purposes, data categories, recipients, cross-border transfers, and profiling activities at the point of data collection. A key challenge is presenting this information in a way that is both comprehensive and comprehensible to users. To balance regulatory requirements with clarity and conciseness in IPCPOs, we aim to understand which information users perceive as most important. This understanding will guide the design of IPCPOs that align with user needs by structuring and prioritizing information based on perceived relevance. Hence, we derive the following research question:

RQ1: Which legally required information should IPCPOs prioritize to balance regulatory obligations with conciseness and perceived usefulness?

User Perceptions of IPCPOs. The adoption of privacy protection tools is influenced by several factors, with response efficacy and privacy concerns being key determinants [17], [18].

Response efficacy refers to an individual's belief in the effectiveness of a tool in mitigating perceived threats. For privacy protection tools such as IPCPOs, it encompasses a user's perception of how well the tool addresses a user's need for information and control over the processing of their personal data. Accordingly, users are more likely to adopt privacy protection tools if they believe they effectively protect their privacy [19]. In this study, response efficacy is broken down into two dimensions: (1) Perceived Transparency, i.e., how clearly and openly the IPCPO communicates data processing details, helping users understand what data is collected and how it is used. (2) Perceived Control, i.e., a user's sense of control over the processing of their personal data.

Privacy concerns refer to individuals' worry regarding the risks of their personal data being misused, accessed without authorization, or exploited for purposes they do not consent to. These concerns influence how users perceive the potential threats to their privacy and motivate them to adopt protective tools like IPCPOs.

Based on these factors, we aim to answer the following additional research questions:

RQ2: How do interactive elements and control features in IPCPOs impact users' perceived privacy control and information efficacy compared to text-based IPCPOs?

RQ3: How do perceived control, perceived transparency, and privacy concerns influence users' intention to adopt IPCPOs?

4.3. Measurement Instrument

For measurement, we adopted established instruments from previous research, tailoring them to the context of our study where necessary. To measure privacy concerns, we used items from Kim et al. [20], adapting them to the Amazon context. For response efficacy, we adapted items from Adhikari and Panda [21] to the IPCPO context focusing on transparency and control. The original English items of the three scales were translated into German following established guidelines [22]. Two independent professional translations were reviewed and refined by two subject matter experts. To measure the intention to adopt IPCPOs, we utilized a validated German translation of the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) [23] questionnaire, specifically adapting the "Intention to Adopt" construct to the IPCPO context on Amazon's e-commerce platform.

4.4. Participant Recruitment and Study Procedure

We recruited participants through the online panel Prolific, selecting a country-specific sample from Germany. We used the Prolific screening filter to ensure that all participants speak

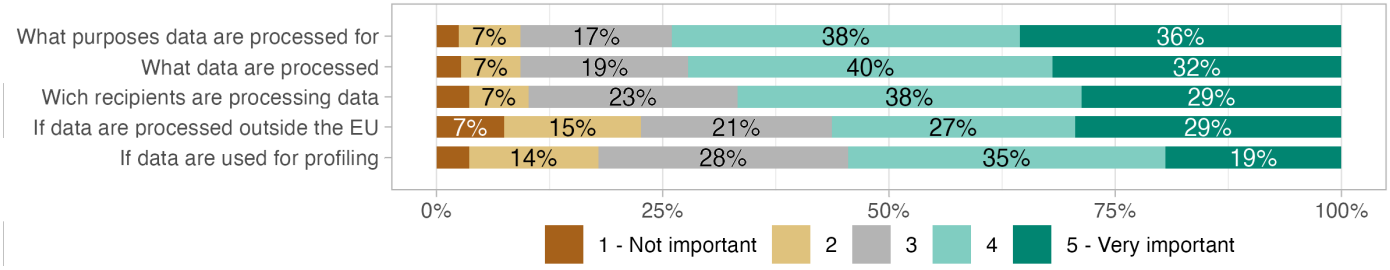

Figure 2: Participants ratings for the relevance of data processing information in the context of an e-commerce platform.

German fluently and to obtain a balanced sample in terms of participants identifying themselves as either female or male. In the study invitation posted on Prolific, we asked participants to test a new feature on Amazon's e-commerce platform.

The study was implemented using a self-hosted instance of LimeSurvey. After obtaining consent, we collected data on participants' frequency of use of Amazon's online shop, their privacy concerns, and their perception of the relevance of different, legally required privacy-related information. Participants were then informed that they would be testing a prototype of a new privacy feature integrated into the Amazon purchase checkout process. We explained the feature using screenshots and provided instructions on how to access the prototype via their smartphone. To this end, participants were randomly assigned to one of three IPCPO prototypes—data-focused, purpose-focused, or text-based—and given a QR code to access the prototype on their smartphone. Depending on their assigned study condition, participants got asked different questions that required them to interact with the IPCPOs. In the data-focused IPCPO condition, participants were tasked with identifying the number of different data categories being processed and determining the purpose associated with processing the postal address. In the purpose-focused IPCPO condition, participants were tasked with identifying the number of different processing purposes and listing the data categories involved in the processing purpose "communication with you." In the text-based IPCPO condition, participants were asked to determine the number of different stated processing purposes. In the data-focused and purpose-focused conditions, participants were also tasked to interact with the privacy settings provided. All study conditions then proceeded to evaluate the response efficacy, and intention to adopt IPCPOs.

5. Results

This section presents the results of our online user study evaluating the data-focused, purpose-focused, and text-based In-Place Contextual Privacy Options (IPCPOs).

5.1. Participant Demographics and Privacy Concern

In total, we recruited 640 participants via Prolific. For data analysis, we excluded participants who failed to answer the attention check question correctly or did not access our prototype via the QR code provided in the study. The final data set consists of 442 valid responses. Our sample is balanced in terms of participants identifying as male (n = 219) or female (n = 223), and is characterized by rather young participants, with a median age of 28 (SD = 9.2). The median duration of the study was 6 minutes. We used Levene's tests for homogeneity [24] to check for deviating variances in the participants' age ($F(2, 439)$ = .584, p = .558) and identifying sex ($F(2, 439)$ = .0160, p = .984) of the three study conditions. The results do not indicate that the random allocation of participants led to unbalanced sub-samples.

In addition, we also ensured that participants' perceived privacy concerns toward Amazon were similarly distributed between the three study conditions. A Shapiro-Wilk test [25] indicated that the response data for privacy concern were not normally distributed. Our measurements resulted in comparable high standard deviations. We presume this relates to divergent perceptions among the participants, which may have been exacerbated by polarizing views regarding the given context of purchasing on Amazon. Taking this into account, we used robust methods in the further analysis. Although the internal consistency of the 'Privacy Concern' construct was marginal (α = .92), it is adequate for a comparison of means. A non-significant Kruskal-Wallis rank sum test [26] indicates that privacy concerns were not unbalanced across the study conditions.

5.2. Relevance of Data Processing Information

We surveyed our participants regarding the importance they attribute to various aspects of data processing when using Amazon's online shop. Participants rated the following topics: (1) the categories of data processed, (2) the purposes for data processing, (3) the data recipients involved, (4) whether data is processed outside the EU, and (5) whether profiling is conducted using the data. Responses were collected on a Likert scale ranging from 1 (Not important) to 5 (Very important).

A Shapiro-Wilk test indicated that the responses were not normally distributed, leading us to employ robust methods to assess differences between the ratings. A heteroscedastic one-way repeated measures ANOVA for trimmed means revealed significant differences among the mean ratings ($F(3.2, 849.29)$ = 22.758, $p < .001$). Subsequent post hoc tests showed no significant differences in the relevance ratings for information about the processed data types, purposes, and involved recipients. Additionally, there was no significant difference in the perceived importance of processing data outside the EU and using data for profiling (cf. Table 1).

Participants rated information about processed data categories, receivers and purposes as more relevant than processing data outside the EU and using data for profiling. Moreover, information about involved recipients was significantly less important than purpose information but not than information on categories of data being processed (cf. Figure 2).

Answering RQ1: Participants find information on processed data categories and processing purposes most relevant, while profiling use and processing of data outside the EU is considered least relevant.

5.3. Comparing IPCPO Variants

To better understand how the three IPCPO variants were perceived, we compared our participants' perceptions of control and transparency, as well as their intention to use a given IPCPO in the future. Shapiro-Wilk tests indicated that the response data were not normally distributed. We therefore conducted Kruskal-Wallis rank sum tests, and if significant, followed up with Dunn tests with Bonferroni corrections for pairwise comparisons. Our findings are reported below.

TABLE 1: Pairwise comparisons of the perceived importance of legally required information on personal data processing.

Comparisons			$\hat{\psi}$	p-value	p_{crit}
Data type	vs	Purpose	-.015	.641	.050
Data type	vs	Recipients	.109	.054	.017
Data type	vs	Non EU	.305	<.001	.007
Data type	vs	Profiling	.384	<.001	.006
Purpose	vs	Recipients	.173	<.001	.013
Purpose	vs	Non EU	.346	<.001	.006
Purpose	vs	Profiling	.399	<.001	.005
Recipients	vs	Non EU	.229	<.001	.010
Recipients	vs	Profiling	.297	<.001	.009
Non EU	vs	Profiling	.068	.288	.025

Response Efficacy Control. The internal consistency of the 'Response Efficacy Control' construct was consistently good across all three conditions (α = .877). A Kruskal-Wallis rank sum test revealed significant differences between the three variants (χ^2 = 28.244, df = 2, p < .005). Pairwise comparisons indicated significant differences between all three prototype variants (cf. Table 3). Specifically, Response Efficacy Control was rated the highest for the data-focused IPCPO (median = 5.00), followed by the purpose-focused IPCPO (median = 4.67), followed by the text-based IPCPO (median = 4.33) (cf. Table 2).

Response Efficacy Transparency. Internal consistency of the 'Response Efficacy Transparency' construct was acceptable for all conditions (α = .768). A Kruskal-Wallis rank sum test revealed significant differences between the three variants (χ^2 = 7.6244, df = 2, p = .022). The pairwise test revealed that perceived transparency was significantly higher for the data-focused IPCPO (median = 5.33) compared to the text-based IPCPO (median = 5.00). However, we did not find any further significant pairwise differences (cf. Table 3). Considering the very small effect sizes (< .1) for non-significant pairwise comparisons, our analysis indicates that the observed differences in perceived transparency are negligible and unlikely to be practically relevant.

Intention to use. The internal consistency of the construct 'Intention to Adopt' was high across all three survey conditions, with a Cronbach's α = .974, possibly due to excessive redundancy among the items. A Kruskal-Wallis rank sum test revealed significant differences in the intention to adopt among the three variants of the IPCPO prototypes (χ^2 = 12.978, df = 2, p = .002). A pairwise comparison revealed that participants' intention to use the data-based and purpose-based IPCPO in the future was significantly higher (median = 5.00) than their intention to use the text-based IPCPO (median = 4.50) (cf. Table 3). However, no significant difference was found between the data-based and purpose-based variants, and the effect size was small, suggesting that participants did not perceive a meaningful distinction between these two variants.

Answering RQ2: Based on the three analyses of perceived control, transparency, and intention to use, we find that the data-focused and purpose-focused IPCPO prototypes were rated significantly higher in response efficacy and intention to use compared to the text-based variant. However, the differences between the data-focused and purpose-focused variants were marginal.

5.4. Factors Influencing Adopting IPCPOs

To assess the impact of perceived transparency, perceived control, and privacy concerns on participants' intentions to adopt IPCPOs, we utilized structural equation modeling (SEM) [27]. We conducted a multi-group comparison to determine whether the three different conditions—data-focused, purpose-focused, and text-based—required distinct models. Specifically, we compared a constrained model (where parameters were held equal across groups) with an unconstrained model. The results indicated that the two models were not significantly different, so we chose to proceed with a single model solution, running SEM on the full dataset without further distinguishing between the different IPCPO prototypes. Due to the non-normality of the data, we used the robust estimator WLSMV. To evaluate the model, we examined several goodness-of-fit indices. The Comparative Fit Index (CFI), the Root Mean Square Error of Approximation (RMSEA), and the Standardized Root Mean Square Residual (SRMR) fell within acceptable ranges, allowing for meaningful interpretation of the results (cf. Table 4). The SEM-based regression analysis identified significant effects of perceived transparency, perceived control, and privacy concerns on participants' intentions to adopt IPCPOs. Notably, the path coefficients highlighted that perceived control has a substantial significant positive effect on users' intention to adopt IPCPOs (β = .381), whereas perceived transparency has a smaller effect (β = .227). Privacy concerns also have a significant effect on intentions to adopt IPCPOs (β = .346). Our results suggest that users' sense of control over data processing and their overall privacy concerns regarding an online service are critical factors influencing their intention to use IPCPOs in practice.

Answering RQ3: Response efficacy and privacy concerns significantly positively influenced participants' intention to use IPCPOs in the future. However, 'Response Efficacy Control' was the primary factor driving this intention.

6. Discussion

In this paper, we introduced the concept of In-Place Contextual Privacy Options (IPCPOs), a transparency-enhancing technology (TET) that integrates visually interactive presentations of privacy-related information and controls directly into the user context, allowing users to take privacy-related actions without interrupting their primary task. We further evaluated and explored user perceptions of a prototype implementation of IPCPOs in an e-commerce context, specifically focusing on how the presentation of privacy details (data-focused, purpose-focused, or text-based) impacts users' perceived control, transparency, and intention to adopt these variants of IPCPOs. We examined the effects of perceived transparency, perceived control, and privacy concerns on users' likelihood of adopting IPCPOs, with the goal of providing insights that can guide the design of privacy features on online platforms.

Prioritizing information. Our findings indicate that users prioritize information about processed data categories and processing purposes, while aspects such as data processing outside the EU and profiling are deemed less relevant. This suggests that privacy interfaces should focus on presenting data types and purposes prominently, while secondary details, such as profiling practices, can be placed in deeper layers of the interface. Notably, participants did not differentiate significantly between data categories, processing purposes, and recipients, reinforcing the idea that these aspects should be grouped together in a way that facilitates user comprehension. In this regard, our study offers valuable insights for developers and designers of transparency-enhancing technologies to empirically determine which information to prioritize in their designs.

Designing for perceived control. We determined that participants' intention to use IPCPOs is primarily influenced

TABLE 2: Summary Statistics for Privacy Concerns, Response Efficacy (RE) and Intention to Use.

	Privacy Concern			RE Control			RE Transparency			Intention to Use		
Condition	Mean	SD	Median	Mean	SD	Median	Mean	SD	Median	Mean	SD	Median
Data	3.72	1.52	3.70	4.92	1.14	5.00	5.27	1.16	5.33	4.84	1.60	5.00
Purpose	4.10	1.50	4.00	4.56	1.30	4.67	5.13	1.19	5.33	5.04	1.61	5.00
Text	4.03	1.36	4.20	3.99	1.51	4.33	4.93	1.26	5.00	4.37	1.70	4.50

TABLE 3: Pairwise comparisons of Response Efficacy Transparency (RE Transparency), Response Efficacy Control (RE Control), and Intention to Use across the study conditions (variants of prototypes).

Comparisons					RE Transparency			RE Control			Intention to Use		
Cond_1		Cond_2	n_1	n_2	Statistic	p_{adj}	Eff. size	Statistic	p_{adj}	Eff. size	Statistic	p_{adj}	Eff. size
Data	vs	Purpose	144	160	-1.497	.403	.085	-2.468	.041	.146	1.163	.734	.069
Data	vs	Text	144	138	-2.759	.017	.165	-5.308	$<.001$	.311	-2.347	.057	.142
Purpose	vs	Text	160	138	-1.349	.532	.078	-3.002	.008	.178	-3.557	.001	.204

TABLE 4: SEM model statistics, fit indices, and regression results.

Model Statistics		Fit Indices		Regression Results			
Metric	Value	Index	Value	Path	Est.	Std. Est.	p-value
Test Statistic	106.469	CFI	.99	Intent. to Use $\sim$ RE Control	.484	.381	$< .001$
Degrees of Freedom	71	RMSEA	.026	Intent. to Use $\sim$ RE Transparency	.387	.227	$< .05$
p-value	$< .005$	SRMR	.035	Intent. to Use $\sim$ Privacy Concern	.384	.346	$< .001$

by their perceived level of control over data processing offered by IPCPOs, in addition to their privacy concerns towards the online service. Perceived transparency had only a small effect. This highlights that designing IPCPOs to enhance perceived control is more critical for adoption than emphasizing privacy concerns or transparency alone.

Participants rated their perceived control higher for IPCPOs with a data-focused design compared to those with a purpose-focused design. This may be because processing purposes are often perceived as either too abstract or, in cases of excessive detail, overwhelming and complex [28].

Interestingly, the higher perceived control in the data-catalog-focused condition seems inconsistent. In the purpose-focused variant, switches for activating and deactivating optional data processing are located at the first level, while in the data-focused variant, users must expand a data category to access these switches on the second presentation layer.

This design aligns with the GDPR's concept of consent to data processing, which is closely tied to specific purposes rather than allowing users to select individual data categories for processing. When a data category is processed alongside a purpose that does not rely on consent, users cannot completely object to processing that category. This creates challenges in providing easy-to-access control functions in data category-focused views and highlights a discrepancy between the GDPR's legislative framework and the preferences of our study participants.

Implementing IPCPOs in practice. Different approaches exist for implementing IPCPOs, one of which is through regulatory frameworks. For one thing, we believe that IPCPOs directly address the common usability challenge in the GDPR of making withdrawing consent as easy as providing consent (Art. 7). Instead of burying privacy settings deep within menus or privacy statements, IPCPOs offer a much-needed alternative by seamlessly integrating privacy controls into a user's primary tasks, making them as accessible and intuitive as other core functionalities of a service. Similarly, the California Privacy Rights Act (CPRA) already mandates an opt-out icon for advertisements and selling data to be present on a data controller's homepage, ensuring users can easily exercise their rights. This highlights the broader potential of regulatory frameworks to implement IPCPOs as a means to ensure users can access privacy controls and information without unnecessary friction.

Beyond regulatory enforcement, there are also strong intrinsic motivations for online services for adopting IPCPOs. Prior research has shown that implementing enhanced privacy mechanisms positively impacts user perceptions of online services, leading to increased trust [29], [30].

7. Limitations and Future Work

While our study provides valuable insights, several factors should be considered when interpreting the findings. Firstly, the sample used in our study was drawn from a German population registered on the Prolific platform. As such, the sample may not fully represent the broader, more diverse user base found on platforms like Amazon. Specifically, the participants in our study tend to be younger and more tech-savvy, as indicated by our demographic analysis. Additionally, restricting participation to German-speaking individuals introduces some cultural context, particularly in terms of privacy concerns, which could influence how participants engage with the study. Secondly, participants interacted with a prototype rather than a fully functional service integrating IPCPOs. This design choice meant that participants did not experience real-world data processing, and thus, our findings primarily reflect short-term evaluations and intentions rather than long-term, real-world usage. Future work should explore how users interact with such systems in frequent, real-world scenarios and how their perceptions evolve over time. Lastly, our statistical analysis, while insightful, was limited by the sample size, which affected effect sizes, especially for between-group comparisons. A larger sample size would help improve the robustness of these findings and allow for more nuanced insights. We acknowledge these limitations to provide a balanced perspective on the results.

8. Conclusions

We introduced and evaluated the concept of In-Place Contextual Privacy Options (IPCPOs), which enable users to access context-specific privacy information and controls without interrupting their primary tasks to review global privacy statements or adjust centralized settings. Our study revealed that users prioritize information on the type of personal data processed, the processing purposes, and data recipients, expressing a preference for visually interactive presentations over purely text-based designs. Furthermore, we found that the intention to use IPCPOs is primarily driven by the perceived level of control they provide rather than the transparency they offer. Our findings indicate that IPCPOs effectively reduce usability burdens even in scenarios involving complex data processing, thereby supporting users in maintaining control over their personal data.

Acknowledgements

Special thanks go to Stefanie Ludborzs for her valuable input on the design of the prototypes. We acknowledge the use of AI-based writing assistants to improve language and grammar in this manuscript. This research was partially funded by the German Federal Ministry of Education and Research under grant number 16KIS1508.

References

[1] R. Chen, F. Fang, T. Norton, A. M. McDonald, and N. Sadeh, "Fighting the Fog: Evaluating the Clarity of Privacy Disclosures in the Age of CCPA," in *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, 2021, pp. 73–102.

[2] J. R. Reidenberg, T. Breaux, L. F. Cranor, *et al.* "Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding." Social Science Research Network: 2418297. (2014), pre-published.

[3] H. Habib, S. Pearman, J. Wang, *et al.*, ""It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu HI USA: ACM, 2020, pp. 1–12. DOI: 10.1145/3313831.3376511.

[4] S. Zhang, L. Klucinec, K. Norton, N. Sadeh, and L. F. Cranor, "Exploring Expandable-Grid designs to make iOS app privacy labels more usable," in *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, 2024, pp. 139–157.

[5] D. Reinhardt, J. Borchard, and J. Hurtienne, "Visual Interactive Privacy Policy: The Better Choice?" In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–12.

[6] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A "nutrition label" for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009, pp. 1–12.

[7] M. Windl, N. Henze, A. Schmidt, and S. S. Feger, "Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–18.

[8] A.-M. Ortloff, M. Windl, V. Schwind, and N. Henze, "Implementation and In Situ Assessment of Contextual Privacy Policies," in *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, 2020, pp. 1765–1778.

[9] Y. Javed and A. Sajid, "A Systematic Review of Privacy Policy Literature," *ACM Comput. Surv.*, 2024.

[10] H. Habib, Y. Zou, A. Jannu, *et al.*, "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites," presented at the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), 2019, pp. 387–406.

[11] M. Bahrini, N. Zargham, A. Wolff, D.-K. Kipker, K. Sohr, and R. Malaka, "It's Long and Complicated! Enhancing One-Pager Privacy Policies in Smart Home Applications," in *Nordic Human-Computer Interaction Conference*, 2022, pp. 1–13.

[12] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, "Standardizing privacy notices: An online study of the nutrition label approach," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 1573–1582.

[13] D. Feth, "Transparency through contextual privacy statements," in *Mensch und Computer 2017 - Workshopband*, 2017.

[14] F. Schaub, R. Balebako, and L. F. Cranor, "Designing Effective Privacy Notices and Controls," *IEEE Internet Computing*, vol. 21, no. 3, pp. 70–77, 2017.

[15] J. Rudd, K. Stern, and S. Isensee, "Low vs. high-fidelity prototyping debate," *Interactions*, vol. 3, no. 1, pp. 76–85, 1996, ISSN: 1072-5520. DOI: 10.1145/223500.223514.

[16] H. Habib, Y. Zou, Y. Yao, *et al.*, "Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–25.

[17] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975. pmid: 28136248.

[18] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology*, vol. 19, no. 5, pp. 469–479, 1983.

[19] A. Chennamaneni and B. Gupta, "The privacy protection behaviours of the mobile app users: Exploring the role of neuroticism and protection motivation theory," *Behaviour & Information Technology*, vol. 42, no. 12, pp. 2011–2029, 2023.

[20] D. J. Kim, M.-S. Yim, V. Sugumaran, and H. R. Rao, "Web assurance seal services, trust and consumers' concerns: An investigation of e-commerce transaction intentions across two nations," *European Journal of Information Systems*, vol. 25, no. 3, pp. 252–273, 2016.

[21] K. Adhikari and R. K. Panda, "Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks," *Journal of Global Marketing*, vol. 31, no. 2, pp. 96–110, 2018.

[22] P. Walde and B. A. Völlm, "The TRAPD approach as a method for questionnaire translation," *Frontiers in Psychiatry*, vol. 14, 2023.

[23] D. Harborth and S. Pape. "German Translation of the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) Questionnaire." (2018).

[24] "R: Levene's Test." (), [Online]. Available: https://search.r-project.org/CRAN/refmans/rstatix/html/levene_test.html (visited on 02/28/2025).

[25] "Shapiro-Wilk Normality Test in rstatix." (), [Online]. Available: https://rdrr.io/cran/rstatix/man/shapiro_test.html (visited on 02/28/2025).

[26] "Kruskal.test function - RDocumentation." (), [Online]. Available: https://www.rdocumentation.org/packages/

stats / versions / 3 . 6 . 2 / topics / kruskal . test (visited on 02/28/2025).
[27] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, "An Introduction to Structural Equation Modeling," in *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*, Cham: Springer International Publishing, 2021, pp. 1–29. DOI: 10.1007/978-3-030-80519-7_1.
[28] L. Kyi, A. Mhaidli, C. T. Santos, F. Roesner, and A. J. Biega, ""It doesn't tell me anything about how my data is used": User Perceptions of Data Collection Purposes," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–12.
[29] F. M. Farke, D. G. Balash, M. Golla, M. Dürmuth, and A. J. Aviv, "Are privacy dashboards good for end users? Evaluating user perceptions and reactions to Google's My Activity," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 483–500.
[30] E. Herder and O. van Maaren, "Privacy Dashboards: The Impact of the Type of Personal Data and User Control on Trust and Perceived Risk," in *Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization (UMAP)*, 2020, pp. 169–174.

Appendix A. Measurement Instruments

A.1. Privacy Concern

Items used to measure privacy concern, adapted from Kim, Yim, Sugumaran, *et al.* [20].

PC1
English: I am concerned that Amazon is collecting too much personal information from me.
German: Ich habe Bedenken, dass auf Amazon zu viele personenbezogenen Daten von mir gesammelt werden.

PC2
English: I am concerned that Amazon will use my personal information for other purposes without my authorization.
German: Ich habe Bedenken, dass Amazon meine persönlichen Daten ohne meine Zustimmung für andere Zwecke verwendet.

PC3
English: I am concerned that Amazon will share my personal information with other entities without my authorization.
German: Ich habe Bedenken, dass Amazon meine persönlichen Daten ohne meine Zustimmung an andere Stellen weitergibt.

A.2. Response Efficacy

Items used to measure response efficacy (adapted from Adhikari and Panda [21]) with translations tailored to transparency and control.

RE1
English: Enabling privacy protection features on Amazon could protect me from information privacy threats.
German: Die Nutzung der neuen Datenschutzfunktionen auf Amazon könnte mich vor Bedrohungen der Privatsphäre schützen.
German focused on transparency: Die Nutzung der neuen Datenschutzfunktion auf Amazon könnte mein Wissen über die Verwendung meiner persönlichen Daten erweitern.
German focused on control: Mit der neuen Datenschutzfunktion auf Amazon könnte ich mehr Kontrolle über die Nutzung meiner persönlichen Daten erhalten.

RE2
English: If I use privacy protection features on Amazon, I am less vulnerable to lose my information privacy.
German: Wenn ich die neuen Datenschutzfunktionen bei Amazon verwende, bin ich weniger anfällig dafür, meine Privatsphäre zu verlieren.
German focused on transparency: Wenn ich die neue Datenschutzfunktion bei Amazon verwende, bin ich weniger anfällig dafür, meine persönlichen Daten preiszugebe, ohne dass ich darüber informiert bin.
German focused on control: Wenn ich die neue Datenschutzfunktion bei Amazon nutze, bin ich weniger anfällig dafür, die Kontrolle über die Verwendung meiner persönlichen Daten zu verlieren.

RE3
English: I can effectively control my information privacy using privacy protection features on Amazon.
German: Ich kann meine Privatsphäre effektiv kontrollieren, indem ich die neuen Datenschutzfunktionen auf Amazon verwende.
German focused on transparency: Mit der neuen Datenschutzfunktion auf Amazon kann ich mich wirksam über die Nutzung meiner persönlichen Daten informieren.
German focused on control: Mit der neuen Datenschutzfunktion auf Amazon kann ich die Nutzung meiner persönlichen Daten wirksam kontrollieren.

A.3. Intention to Adopt

Items to measure the intention to adopt, adapted from Harborth and Pape [23].

ITA1
German: Ich beabsichtige, in der Zukunft auch weiterhin die neue Datenschutzfunktion zu nutzen, wenn diese angeboten wird.

ITA1
German: Ich werde im Alltag immer versuchen, die neue Datenschutzfunktion zu nutzen, wenn diese angeboten wird.

ITA1
German: Ich habe vor, weiterhin regelmäßig die neue Datenschutzfunktion zu nutzen, wenn diese angeboten wird.

Appendix B. Prototype Implementation

An implementation of the prototype as used in this study can be found at: https://github.com/das-group/IPCPO-Prototype.