"*Summar*": Simplifying Privacy Policies of E-commerce Websites

Jasmine Ly
York University

Prachi Sadhwani
York University

Ian Galendez
York University

Abstract

Millions of people interact with e-commerce platforms, like Amazon, SHEIN, and Temu, on a daily basis. However, few users admit that they can understand the privacy policies of these e-commerce retailers, and fewer admit to have read them. We developed *Summar*, a Google Chrome extension that summarises the privacy policies of various e-commerce platforms to address the privacy implications that arise between an online retailer and the user. Twelve participants participated in a usability study, followed by a brief semi-structured interview and survey. Our study sheds light upon the development of browser extensions to promote privacy and safety. Based on our findings, users expressed interest in the ability to condense lengthy privacy policies, but found it difficult to maintain engagement with such tools. While the study focuses on e-commerce websites, our findings may be applied in other fields within the web extension development sphere.

1 Introduction

Since the COVID-19 pandemic in 2020, many people across the globe have found themselves resorting to purchasing commodities online, through e-commerce websites [21]. Particularly, studies have shown that individuals between the ages of 18-25 look for the cheapest and most convenient methods to obtain the products they desire [14]. However, countless users fail to realise exactly how much information and what kind of data they are providing these e-commerce retailers upon interacting with them [16, 19]. Furthermore, users do not have a complete understanding of the threats to security and privacy that come with the collection of their data [16]. Instead, users have the misguided belief that companies are protecting their data more than they are, simply due to the fact that a privacy policy is required by the law.

Generally, users fail or refuse to comprehend the privacy notices and terms of service agreements presented to them when they begin using these e-commerce websites for numerous reasons, including the fact that privacy notices tend to be too long and inconvenient for users to read. Moreover, they include a variety of complex, legal terminology and are strategically placed out of the user's central focus [19].

Despite not having a complete understanding of the privacy notices and terms of service (as well as the risks associated with the use of these platforms), many users still accept them. This is not necessarily the fault of the user, but often the result of "deceptive design patterns" [3].

Deceptive design (sometimes referred to as dark patterns) refers to the use of manipulative and distracting elements in user interfaces to intentionally trick users into making choices that they are not fully aware of [4]. With the recent and rapid growth of the data economy, there exists an abundance of platforms that employ deceptive design elements to exploit users for their information, the major culprits being e-commerce giants such as [20]:

- Amazon[1] - for general lifestyle, grocery, and technology-related goods.
- Temu[2] - for general lifestyle and technology-related goods.
- SHEIN[3] - for fashion and lifestyle goods.

Consequently, our objective is to analyse and understand the deceptive design strategies that e-commerce retailers use in order to get users to agree to their privacy notices. Using our findings from this analysis, we decided to create a tool that encourages users to read and understand what data they are voluntarily giving to these companies by summarising the privacy policies. This tool allows users to bypass these intentionally malicious, dark patterns and have a clear and simple overview of the contents of the privacy notices and terms of service agreements. Through this study, we answered the following research questions:

[1] https://www.amazon.ca/
[2] https://www.temu.com/ca/
[3] https://m.shein.com/ca/

RQ1: How are e-commerce retailers deploying deceptive design to manipulate users into blindly accepting privacy policies?

RQ2: How may we develop a browser extension to improve user privacy on e-commerce retail websites?

RQ3: Do users find this kind of browser extension useful when interacting with these e-commerce websites?

Currently, there are not many affordable tools available to the general public that summarises and simplify privacy policies effectively. Instead, there exists a multitude of software that provide the user with a rating for a platform's privacy policy or block unwanted/malicious trackers[4]. With the development of this tool, we hope to create an effective and affordable solution to the issue of deceptive design and the inaccessibility of privacy notices.

To create our tool, we first conducted an extensive literature review to understand how these e-commerce retailers use deceptive design patters to entice users to browse through their websites, sign up for their services, and purchase items without understanding the personal privacy implications. Simultaneously, we reviewed the privacy notices of the aforementioned popular e-commerce giants. We then combined the results of these analyses to design and develop a Google Chrome extension, conducting a usability study to understand user perceptions of the browser extension and gain feedback as to how it can be improved.

2 Background

Previous literature has explored the reasons behind users' reluctance and avoidance of reading privacy notices. In this section, we will explore the cognitive and legal reasoning behind the lack of understanding of privacy notices. Furthermore, we will explore how e-commerce websites use deceptive design in order to manipulate users into sharing more data and private information than they originally intended to.

McDonald et al. [13] found that it would take the average American user approximately 244 hours to read and understand the content of major privacy policies on the web. Additionally, these policies require a college/university-level education to be able to completely understand its contents [19]. However, these are statistics established over six years ago. More recent research has found that these policies have only gotten longer and less readable for the average user, with the inclusion of legal jargon and ambiguous language [18]. Modern privacy policies are asymmetrical in terms of the information conveyed to the user – they know less and less about the details of what data they are voluntarily sharing with the company and how that data will be processed and used in the future [11].

[4] https://chromewebstore.google.com/search/privacy

This is primarily because privacy notices are typically not written for the benefit of the user, but rather they are written for the legal benefit of the company/corporation implementing them [5]. Privacy laws mandate the existence of a notice and consent policy but has no restrictions or regulations as to how the content of the policy is conveyed or explained to the user [19]. Moreover, most companies employ an "opt-out" policy which requires users to explicitly reject abiding by the privacy policy rather than explicitly accepting them [5].

Corporations use the complexity of privacy policies to exploit the user in combination with deceptive design elements. Deceptive design or deceptive patterns refers to aspects of design that are specifically created in order to manipulate the user into making a choice that benefits the corporation (or third parties) more than themselves. These design elements are more likely to be featured on e-commerce websites, where users are at a higher risk of being financially manipulated. While numerous studies have been dedicated to classifying deceptive patterns and creating taxonomies, we will be focusing on "preselection" patterns [3] and "forced action/enrolment" patterns [11].

Preselection patterns refer to designs where the default is selected for the user, which influences their decision-making processes [3]. This can be clearly seen in Figure 1 where a user decides to sign up for a new service, the option to accept the Privacy Notice and Terms of Service is pre-selected for them.

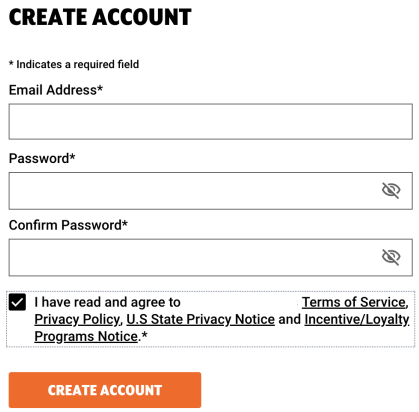

Figure 1: An example of Preselection deceptive patterns.

The above-mentioned example works for the following reasons. The lengthiness and language of privacy notices require users to spend an excessive amount of their cognitive resources in order to make a decision [5]. This facilitates the acceptance of the default option of accepting the privacy policy without actually reading through it. This has been previously described as the "status quo bias" or "default bias" [2]. Individuals not only choose the default out of "laziness"

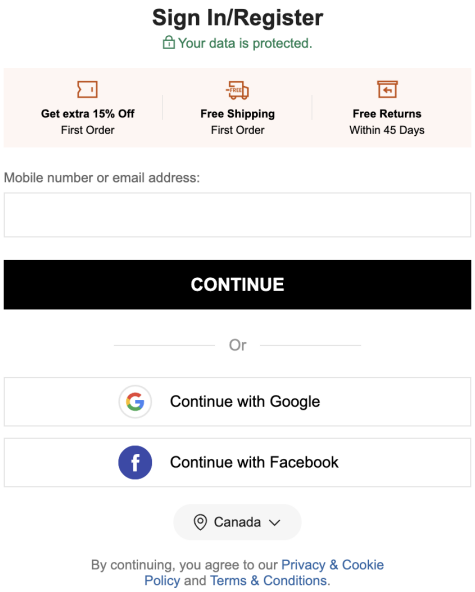

Figure 2: An example of Forced Action deceptive patterns.

or cognitive exhaustion but also because they assume that it is the best option for them (possibly because the default option inflates its attractiveness [19]).

Forced action patterns occur when the user is presented with something they want but the website requires them to do something in return [7]. Typically, this is seen when users want to purchase something from an e-commerce retailer but the website forces them to sign up for their services prior to checking out. Figure 2 is an example from SHEIN, one of the websites we focused on for *Summar*.

For all three e-commerce websites we explore in this paper, users automatically accept their privacy policies by completing the sign-up process. Additionally, the privacy policy and terms of service agreements are hidden behind small hyperlinks which lead to complex and convoluted walls of text. This causes users to be unaware of the data they are sharing with these companies, a situation often referred to as "privacy Zuckering" [12].

Utz et al. [17] identified and investigated the common properties of consent notices to find that the size, position, and framing of choices involved have a significant influence on the decision that a user makes. Position and choices presented have more of an effect on users than the content or presence of hyperlinks to additional information. For Amazon, Temu, and SHEIN, these notices take up minimal design space and do not seem to provide the user with any choice of acceptance.

It is essential to inform users about the data that these companies are collecting and provide them with details regarding how this information is stored and used. Many scholars argue that it is a user's right to know and understand where their information is going, especially with the rapid growth of the data economy [19]. Without this information, users are at risk of being exploited and making harmful decisions relating to their privacy and digital security. Additionally, Tsai et al. [15] found that users are more likely to purchase commodities from online retailers who they perceive to protect their privacy better. This indicates that both consumers and retailers will benefit from the effective communication of privacy policies.

Prior scholarship has suggested solutions that will improve the usability of privacy policies. Acquisti et al. [2] suggested that reforming the language to be more understandable for the average user will increase the likelihood of users reading a policy. Kelly et al. [10] explored the concept of employing a "nutrition label" design for privacy policies and found that participants could find and retain privacy-related information better with the label approach than with the current, widely adopted natural language policies. Finally, many papers [1, 2, 6] focus on the creation of automated nudge tools to encourage users to make more privacy-conscious decisions.

We took these findings and suggestions about privacy policies and dark patterns into consideration, and further decided to develop a browser extension that would simplify and summarise the contents of privacy policies. We call this extension "*Summar*" (based on the term *'summary'*). The following sections detail the process of designing, developing and testing our extension.

3 Designing and Developing *Summar*: The Privacy Policy Assistant

We developed a web browser extension called *Summar*[5] (built with Google Chrome's browser extension API) that simplifies the privacy policies of various e-commerce websites. We created *Summar* with the intention that retailer policies will be readily accessible, no matter the user's familiarity with data security or privacy.

The design for *Summar* (as seen in Figure 3) follows human-computer interaction design principles to deliver a bullet-point formatted summary of such policies within a user-friendly interface. For the first iteration of our design, we used industry-standard User Interface (UI) design patterns. Specifically, we implemented a two-panel selector so users can navigate the compounded information. To provide a summary that is palatable for all users, we divided the information into the following four categories:

> **Collection:** *Summar* identifies what is required from the user in exchange for the services of the e-commerce website. This includes account creation and management,

[5] https://github.com/prach19/jades-4441

fulfilling and processing orders, customer support, and marketing endeavours.

User Rights: This section describes what users can do to manage the data that is collected from them. Resources are provided to direct the user on how to opt-out, and to what extent, as outlined in the terms of service of the selected e-commerce retailer. *Summar* identifies the extent in which users may opt out of data collection practices before breaching the retailer's termination of service.

Retention: This section outlines how long the user's data is being kept. *Summar* highlights if the information provided within the privacy policy is vague, or omitted.

Storage: *Summar* summarises where user data is being stored, and if the retailer is processing and sending data outside the user's country.

Figure 3: *Summar*'s interface on SHEIN's landing page. The user is viewing how SHEIN retains their data under the "Retention" tab.

4 Methodology

Twelve participants participated in our usability study, which was followed by a semi-structured interview. The participants were recruited through posts on social media (primarily Instagram and Discord) and snowball sampling. The participants were young adults in university, aged between 18 and 25, who had prior experience with e-commerce websites, with the common purpose being online shopping or browsing. We aimed to recruit participants from three audiences: Psychology/Law students, Computer Science/Technology students, and students in other university majors to get a better understanding of how perceptions can differ when an individual has different educational backgrounds/fields. Table 1 summarises the relevant information about participants. Each participant completed a consent and general information form before attending their session. Each session lasted approximately half an hour. No compensation was provided for participation.

Participant	Gender	Education Major
P1	Man	CompSci/Tech Adjacent
P2	Man	Other Major
P3	Non-Binary	Psychology/Law Adjacent
P4	Woman	Other Major
P5	Man	CompSci/Tech Adjacent
P6	Man	CompSci/Tech Adjacent
P7	Woman	Psychology/Law Adjacent
P8	Woman	Psychology/Law Adjacent
P9	Woman	CompSci/Tech Adjacent
P10	Woman	Psychology/Law Adjacent
P11	Woman	Other Major
P12	Man	Other Major

Table 1: List of participants and university majors.

At the beginning of each session, participants were informed that they were participating in a study about e-commerce websites and privacy. Participants were aware that a browser extension had been developed for the study, but were offered no further instructions beyond navigating the e-commerce websites as they normally would. This ensured that users would use *Summar* as they naturally would in their daily lives. Participants were requested to think out loud as they traversed Amazon, SHEIN, and Temu with the *Summar* extension running on their web browser. The order in which the participants accessed all three websites was counterbalanced to ensure there were no order effects or recency bias – the participant's opinion would not be influenced by which privacy policy they read first. The semi-structured interview was conducted afterwards to understand how familiar the participants were with e-commerce websites, their perceptions of the privacy policies, and to gather the participants' thoughts on using assistant applications like *Summar* in their daily lives. The sessions were conducted remotely on *Zoom* for communication and transcription. Participants controlled the interviewer's browser that had *Summar* installed using *TeamViewer*. All data was stored in a Google Drive folder, only accessible to the researchers.

The transcripts of each session were first analysed by all three researchers. Two researchers then coded the data to identify common themes. To maintain consistency in the coding process, the first four interviews were coded by one researcher

and the remaining interviews were coded collaboratively. The following section highlights key results from our analyses.

5 Results

The researcher conducting each session took notes as participants completed the given tasks. Afterwards, the recordings and transcripts of each session were reviewed again to refine our observations. Notes were divided into the following ten categories:

- On a scale of 1 to 5 (with 1 being least familiar, 5 being most), how comfortable the participant was with using e-commerce websites,
- If the participant has read the privacy policies of e-commerce websites before,
- What the participant learned from using *Summar* that they did not know previously,
- Participant's perceptions of e-commerce websites, including any changes in their perception after using *Summar*,
- What participants liked about *Summar*,
- What the participant disliked about *Summar*,
- On a scale of 1 to 5 (with 1 being that the participant was the least content with the information provided by *Summar*, and 5 being the most content) how the users felt about the summarised privacy policies *Summar* offered for the e-commerce websites we had them navigate through,
- And if the participant would use *Summar* again in their daily lives.

After the session notes were compiled, they were organised onto a spreadsheet. The group average and median were calculated, and sentiments expressed among participants were colour coded to identify common themes.

All twelve participants stated they had experience using at least one of the e-commerce websites explored in this study, with a group average rating of 4.375 and group median of 4.25 for familiarity. Two participants acknowledged the possibility of companies being able to commit "shady" practices behind their privacy policies, however, only one participant reported to have read the privacy policies of e-commerce websites before. P12 stated that though he had briefly read on privacy policies before, he trusted the government to keep him safe. P2 said that the only experience in reading privacy policies were the End-User License Agreement (EULA) for games, albeit, he admits to mostly skimming them. Likewise, P10 does not read privacy policies because "*everyone else [doesn't], and nothing bad has happened to [anyone]*", despite later recounting a story that her brother told her about Temu selling information and subsequent security breaches. Three participants cited the inaccessibility of privacy policies as their reason for not reading them. From this, we can conclude that users are aware that companies can use privacy policies as a way to take advantage of the customer. The inaccessibility of privacy policies coupled with the vague understanding of the privacy implications deters users from reading them because they feel that there is no urgency or incentive to do so.

Every participant had expressed they learned something new after interacting with *Summar* across Amazon, Temu, and SHEIN. For some participants, these discoveries had challenged their preconceptions of these three companies. P1 thought that SHEIN was based in Canada, and so initially placed more trust in SHEIN over other companies like Temu. After using *Summar*, P1 was alarmed by SHEIN's privacy policies, especially with regard to its retention of data overseas. For P7, she was surprised to learn that companies, particularly Amazon, disclose her account to the government. A few participants had stumbled upon terminology and data practices, they were unfamiliar with.

"*SHEIN doesn't allow us deleting our own information?*" P1 was glad to have learned more about SHEIN. "*I won't be shopping with them again.*"

"*There is nothing I can do to stop them using or withholding my information, which sucks*," P9 said with regard to SHEIN, but was relieved to know that, after reading over the *User Rights* category, she could request to have her information removed.

"Why does Amazon keep mentioning Washington laws? I live in Canada," stated P1 after reading about their rights when using Amazon's website.

Every participant encountered certain terms and concepts that confused them or upset them. Table 2 further summarises these points of confusion.

Three of the participants expressed after using *Summar* that they felt more informed of their rights as a customer. Seven reported that they were not previously aware of the ways in which e-commerce retailers were retaining their data. SHEIN's privacy policy states that customer data may be kept for fraudulent activity. P6 remarked that they did not know what "fraudulent activity" entailed, and wished there was a clear definition in the policy.

Generally, the participants were satisfied with *Summar*. The group averages were: 3.54 satisfaction for Amazon, 3.75 satisfaction for Temu, and 3.63 satisfaction for SHEIN (see Figure 4). Likewise, the group medians were 3.75 satisfaction Amazon, 4 for Temu, and 4 for SHEIN. Five participants stated that they enjoyed the simplicity of *Summar* and the categorical organisation of data. Two participants said that *Summar* was visually appealing. Two participants highlighted *Summar*'s

Participant	Number of Confusions	Confusion Point
P1	3	Retention as necessary, Anonymization, Washington laws
P2	3	Consent mechanisms, Retention policies, State law references
P3	1	Legal exemptions
P4	1	Data deletion timelines
P5	3	International data transfers, Legal exemptions, Washington laws
P6	1	Withdrawal of consent as necessary
P7	1	Third-party sharing
P8	2	Anonymization, Retention as necessary
P9	2	Sensitive data, Retention policies
P10	3	Indexed data, Cookies, Washington laws
P11	2	Legal justifications for data use, International transfers
P12	3	Anonymization, Legal exemptions, State-specific policies

Table 2: Confusion each participant experienced from the condensed privacy policies provided by *Summar*

accessibility and ease of use, and one participant remarked that they enjoyed how the extension immediately appeared as soon as they entered a specific web page, stating it felt like a warning label.

Conversely, a common sentiment between all participants was that the presentation of the data needed to be improved, such as the typeface, size of the text, and paragraph spacing. P1 noted that they wished the extension deployed simpler terms in the summaries. Though only half of the participants said that they could imagine themselves using an extension like this in their daily lives, most recognised the usability of this extension for people who were not as "tech-savvy" or digitally literate (see Figure 5). P8 and P5 felt they could recommend *Summar* to more vulnerable people such as those in older generations. P4 felt that they would only use *Summar* on a situational basis, like in the case of accessing websites for the first time. P3 and P9 expressed interest in using a tool like *Summar* to compare the privacy policies of different websites.

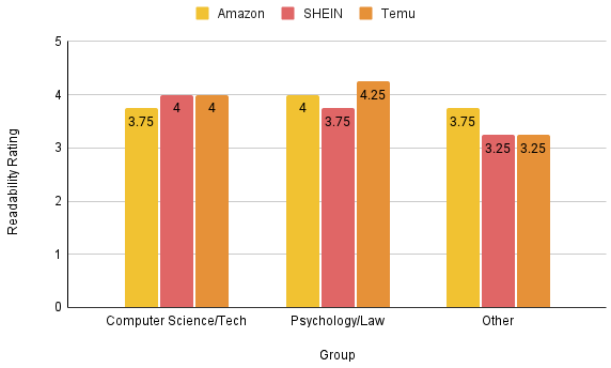

Figure 4: Participant ratings of readability.

Interestingly, each educational background group of partic-

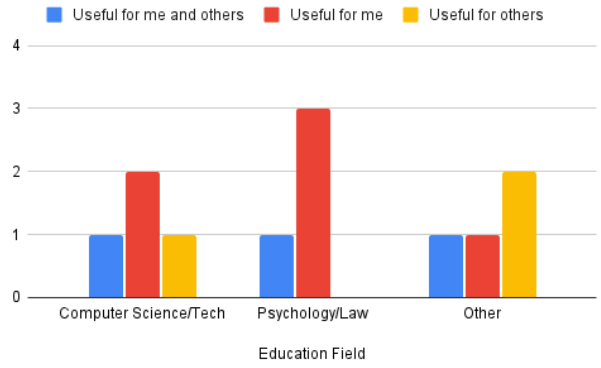

Figure 5: Participant ratings of usefulness.

ipants had different concerns when it came to the design and functionality of *Summar*. Data in Figure 4 shows that the Psychology/Law group generally rated the readability of *Summar*'s summaries higher than other groups, which was expected as individuals in those fields deal with complex, legal and scientific terminology more often. Participants in the Computer Science/Technology related majors found more issues with the UI design rather than the content. On the other hand, participants that came from other fields (including Psychology and Law) found that the amount of text within the browser extension was, at times, overwhelming and suggested condensing it further. These participants also believed that there was no incentive to read the simplified/summarised privacy policies if there was nothing they could do to protect themselves.

6 Discussion

Overall, most participants found the employment of a browser extension to simplify privacy policies to be useful, but not

for their personal use specifically. Participants expressed that this tool would be more useful for vulnerable individuals. We suspect that this could be the result of optimism bias, where users believe that they are more aware of privacy threats and therefore less susceptible to them [9]. As a result, these individuals are more likely to exhibit riskier behaviours and more likely to be affected by some kind of privacy breach.

Due to time constraints, our study had a limited pool of participants. Consequently, our results are primarily applicable to university students. Additional research with a larger, more diverse sample would be required to determine the usability of *Summar* for the general population. This sample would include people from different cultural backgrounds, education levels, and experience with e-commerce websites. Such research is crucial to further understanding how we can develop effective and accessible tools for the growing population of people who turn to e-commerce retailers for all their purchasing needs.

Major improvements to the visual design of the extension would be required before *Summar* is ready to be a publicly accessible tool. While we received feedback for changes concerning the typeface and size of text, we consider that improvements on the colour scheme may be required since colour can have an unintended effect on user behaviour [8]. Future research and development could investigate the possibility of allowing users to customize the appearance of content in a way that is more comprehensive for them. A customisable tool would ensure that a larger population would be able to use it, since information representation would be tailored to the individual person, regardless of their digital literacy and experience. This would probe further concerns about the extent to which a user can customise the extension. However, we acknowledge that no tool is universally applicable and there will always be concerns when we attempt to balance accurate and concise content with attractive and appealing design.

A major limitation for browser extensions that we foresee is the fact that users would need to download the extension from the appropriate web store in order to use it. This would require them to be somewhat informed and concerned about the privacy implications of using e-commerce websites. Based on our findings, many users are not currently concerned about their privacy when browsing e-commerce websites. Thus the usefulness of such a tool is almost entirely reliant on the users' preconceived perceptions and beliefs about privacy.

Moreover, *Summar* can only inform users about the content of privacy policies, but we do not highlight what users can do in order to protect themselves. According to our findings, we have identified that the participants have a vague understanding of the privacy implications and risks associated with these policies. While participants have an idea as to the ways in which companies may deploy their policies to take advantage of the user, they believed these risks apply to more vulnerable groups of people. Thus, coupled by the fact that the presentation of privacy policies are inaccessible, users are generally dismissive of privacy policies. For all three websites, the most privacy conscious decision a user can make is to not interact with or purchase anything from them. Most users potentially overlook any privacy threats because online shopping allows for convenient and cost-effective purchasing. While this may differ depending on the user and their level of digital literacy, the effectiveness of *Summar* is limited to the user's willingness to sacrifice convenience and low prices to keep their information and data private.

As previously mentioned, we believe that this extension can be developed further to apply for a wide variety of e-commerce websites. However, in doing so, beyond improving users' perceptions of the negative privacy implications of privacy policies, we would need to employ machine learning models and artificial intelligence (AI) plug-ins to create an effective tool. This comes with a different set of concerns as users may be hesitant to trust a tool that is supported by AI.

Further research would be required to determine how useful a browser extension would be for general internet browsing. Previous research into nudges [1, 2] has shown that the design and context of the nudge is essential to its effectiveness. Users may ignore them or resist them if they do not trust the source. We believe that these findings also apply to browser extensions like *Summar* because they act as a kind of nudge.

Similarly, the ethical considerations of such a browser extension must be considered. Encouraging users to make more privacy conscious decisions can be seen as a way of manipulating them into making certain decisions. Following Acquisti et al. [2], the development of browser extensions would require a kind of ethical framework to ensure that users are making informed decisions on their own, without external influences.

7 Conclusion

With the growing use of e-commerce platforms, it is essential that users understand the privacy implications of doing so. Consequently, we have designed and developed a Google Chrome browser extension named *Summar* that summarises and simplifies the content of privacy policies for three major e-commerce retailers: Amazon, SHEIN, Temu. In order to determine the usefulness and effectiveness of such a tool, we conducted a usability study with 12 participants from varying educational backgrounds. Overall, most of the participants found the tool to be useful but stated that it needed additional design improvements before being published. While such a tool can be seen as useful, we acknowledge that there are ethical and practical concerns that come with its employment. Future research can focus on addressing these concerns while

further developing *Summar* to be more accessible and readable.

References

[1] Alessandro Acquisti et al. “Nudges (and deceptive patterns) for privacy: six years later”. In: *The Routledge Handbook of Privacy and Social Media*. Routledge, 2023, pp. 257–269.

[2] Alessandro Acquisti et al. “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online”. In: *ACM Comput. Surv.* 50.3 (Aug. 2017). ISSN: 0360-0300. DOI: 10.1145/3054926. URL: https://doi.org/10.1145/3054926.

[3] Brignull et al. *Deceptive patterns – user interfaces designed to trick you*. Apr. 25, 2023. URL: https://www.deceptive.design/.

[4] Weichen Joe Chang, Katie Seaborn, and Andrew A. Adams. “Theorizing Deception: A Scoping Review of Theory in Research on Dark Patterns and Deceptive Design”. en. In: *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, May 2024, pp. 1–7. ISBN: 9798400703317. DOI: 10.1145/3613905.3650997. URL: https://dl.acm.org/doi/10.1145/3613905.3650997.

[5] “Defaults, Framing and Privacy: Why Opting In-Opting Out”. In: *Marketing Letters* 13.1 (2002), pp. 5–15. ISSN: 09230645, 1573059X. URL: http://www.jstor.org/stable/40216617.

[6] Paul Graßl et al. “Dark and Bright Patterns in Cookie Consent Requests”. In: *Journal of Digital Social Research* 3.1 (Feb. 2021), pp. 1–38. ISSN: 2003-1998. DOI: 10.33621/jdsr.v3i1.54. URL: https://publicera.kb.se/jdsr/article/view/24973.

[7] Colin M. Gray et al. “The Dark (Patterns) Side of UX Design”. In: CHI ’18. Montreal QC, Canada: Association for Computing Machinery, 2018, pp. 1–14. ISBN: 9781450356206. DOI: 10.1145/3173574.3174108. URL: https://doi.org/10.1145/3173574.3174108.

[8] Richard H Hall and Patrick Hanna. “The impact of web page text-background colour combinations on readability, retention, aesthetics and behavioural intention”. In: *Behaviour & Information Technology* 23.3 (2004), pp. 183–195. DOI: 10.1080/01449290410001669932. eprint: https://doi.org/10.1080/01449290410001669932. URL: https://doi.org/10.1080/01449290410001669932.

[9] Barbara Hewitt and Garry L. White. “Optimistic Bias and Exposure Affect Security Incidents on Home Computer”. In: *Journal of Computer Information Systems* 62.1 (2022), pp. 50–60. DOI: 10.1080/08874417.2019.1697860. URL: https://doi.org/10.1080/08874417.2019.1697860.

[10] Patrick Gage Kelley et al. “A "nutrition label" for privacy”. en. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. Mountain View California USA: ACM, July 2009, pp. 1–12. ISBN: 9781605587363. DOI: 10.1145/1572532.1572538. URL: https://dl.acm.org/doi/10.1145/1572532.1572538.

[11] Arunesh Mathur et al. “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites”. In: *Proc. ACM Hum.-Comput. Interact.* 3.CSCW (Nov. 2019). DOI: 10.1145/3359183. URL: https://doi.org/10.1145/3359183.

[12] Symran Bhue Mazumdar Stuti. *Responsible Design Part 10 of 14: Privacy Zuckering*. en-US. May 2022. URL: https://think.design/blog/responsible-design-part-10-of-14-privacy-zuckering/.

[13] Aleecia M. McDonald and Lorrie Faith Cranor. “The Cost of Reading Privacy Policies”. In: *I/S: Journal of Law and Policy for the Information Society* 4.3 (2008), pp. 543–568. URL: https://heinonline.org/HOL/P?h=hein.journals/isjlpsoc4&i=563.

[14] Aaron Smith and Monica Anderson. *Online Shopping and E-Commerce*. en-US. Dec. 2016. URL: https://www.pewresearch.org/internet/2016/12/19/online-shopping-and-e-commerce/.

[15] Janice Y. Tsai et al. “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study”. In: *Information Systems Research* 22.2 (2011), pp. 254–268. DOI: 10.1287/isre.1090.0260. eprint: https://doi.org/10.1287/isre.1090.0260. URL: https://doi.org/10.1287/isre.1090.0260.

[16] Joseph Turow, Michael Hennessy, and Nora Draper. “Persistent Misperceptions: Americans’ Misplaced Confidence in Privacy Policies, 2003-2015”. eng. In: *Journal of Broadcasting & Electronic Media* 62.3 (2018), pp. 461–478. ISSN: 0883-8151.

[17] Christine Utz et al. “(Un)informed Consent: Studying GDPR Consent Notices in the Field”. en. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. London United Kingdom: ACM, Nov. 2019, pp. 973–990. ISBN: 9781450367479. DOI: 10.1145/3319535.3354212. URL: https://dl.acm.org/doi/10.1145/3319535.3354212.

[18] Isabel Wagner. *Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996–2021*. 2022. DOI: 10.48550/ARXIV.2201.08739. URL: https://arxiv.org/abs/2201.08739.

[19] Ari Ezra Waldman. "Privacy, Notice, and Design". In: *Stanford Technology Law Review 21 Stan. Tech. L. Rev. (2018) LibGuide* 21 (2018), pp. 74–126. URL: https://heinonline.org/HOL/P?h=hein.journals/stantlr21&i=74.

[20] Similar Web. *Top E-Commerce & Shopping Websites Ranking - October 2024*. https://www.similarweb.com/top-websites/e-commerce-and-shopping/. 2024.

[21] Salim Zanzana and Salim Martin. *Retail e-commerce and COVID-19: How online sales evolved as in-person shopping resumed*. Apr. 25, 2023. URL: https://www150.statcan.gc.ca/n1/pub/11-621-m/11-621-m2023002-eng.htm.

Appendix

Participant Demographic Information Form

1. Name:
2. Email:
3. Gender Identity:
   - Man
   - Woman
   - Non-Binary
   - Other:
   - Prefer Not to Say
4. Which of the following e-commerce websites have you used before?
   - Amazon
   - SHEIN
   - Temu
   - Other:
5. Please confirm the following:
   - I confirm that I am young adult (between the ages of 18-25).
6. Please select which category best describes your major:
   - Computer Science/Technology or Adjacent
   - Psychology/Law or Adjacent
   - Other:
7. My session date and time is:
8. Please confirm the following:
   - I will have Zoom AND TeamViewer installed prior to my session time.

Study Script

- This study is designed to see how people react to our browser extension for our study. We will have you go through three e-commerce websites in a specific order and we will observe what you do as you are traverse the website.
- We will notify you when it is time to move on to the next website. Once you have completed going through all three websites, we will then move on to the interview portion.
- As you are completing the objective, we would like you to think out loud to help us understand what you are doing and your reasoning for the same. This experiment will last approximately 30 minutes.
- Do you have any questions?

Interview Script

- Have you used any of these e-commerce websites site before?
- On a scale of 1 to 5, how comfortable are you with navigating these websites?
- Have you read the privacy notices for any of these e-commerce websites before this study?
- Did you learn something new about privacy policies by using this extension?
- Has your perception of privacy on e-commerce websites changed through the use of this extension?
- What did you like most about the extension?
- What did you dislike about the extension?
- On a scale of 1-5, how would you rate the readability of the information in the browser extension on each website?
- Do you see yourself using this extension in regular life? With other e-commerce websites?