International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. 12, Issue 5, May 2024

https://ijecm.co.uk/

A STUDY ON EXPLORING THE IMPORTANCE OF AWARENESS ON ONLINE PRIVACY ACCEPTANCE

Erjonilda Hasrama
University “Aleksander Moisiu”, Durres, Albania
nildakajo@yahoo.com

Abstract

In the digital age, privacy policies serve as crucial documents for informing users about how their personal data is collected, processed, and protected by online platforms. However, the effectiveness of these policies in fostering user trust and awareness is not performed uniformly across websites, highlighting the need for further investigation into factors influencing user perceptions and behaviors regarding privacy practices online. This study aims to investigate the privacy practices of e-commerce websites in Albania, focusing on the accessibility, structure, and comprehensibility of their privacy policies, as well as their impact on user perceptions and trust. Through a mixed-methods approach, including manual analysis of privacy policies and an experimental study with university students, this research explores the objective and subjective elements of privacy policies and their influence on user perceptions and intentions. Participants were randomly assigned to groups exposed to high or low-rated privacy policies, and their responses were analyzed to gauge perceptions of trust, transparency, and data control. The findings reveal that while many websites prioritize transparency in their privacy policies, gaps exist in addressing user data control and security measures. Websites with clear, accessible, and user-friendly privacy policies are perceived more positively by users, leading to higher levels of trust and intention to interact with the platform. Notably, the inclusion of anthropomorphic elements in privacy policies appears to influence users' disclosure of personal information. Moreover, gender differences in privacy awareness highlight the need for tailored communication strategies.

Keywords: Privacy policy, GDPR, Privacy awareness, Trust, Transparency

INTRODUCTION

People may not purchase something from a company because they weren't sure how their personal information would be used (Ackermann et al. 2021). Privacy policies are often challenging for consumers to understand due to their complex language and written in professional format (Ravichander et al. 2021) and even the increase in prevalence of privacy policies, people rarely read them (Steinfeld, 2016). Privacy policies differ, significantly, from websites and even from apps, making it sometimes difficult to compare the information contained in them. Given that privacy policies are often not thoroughly read by users, individuals may unintentionally misunderstand the terms outlined within them (Kroger et al. 2021).

According to Tsai et al. (2007) many people express concerns about their online privacy, particularly when shopping on the internet. However, most individuals do not read privacy policies thoroughly and instead only notice their presence. This suggests that accessing privacy information remains difficult, leading many to bypass reading policies and hope for the best. Despite this, people generally hold realistic views about the likelihood of their online behavior being tracked by websites to infer information about them. Many studies states that most of the individuals explain that they are concerned about online privacy and that the disclosure of personal information is important to them however, they are not keen to read or understand what they are approving (Spiekermann et al. 2006). The clarity and accessibility of online privacy policies impact individuals' ability to understand them. Policies that are well-organized, concise, and presented in plain language are more likely to be comprehensible to a wider audience. Contrary, complex policies can discourage individuals from engaging with them (Reidenberg et al. 2015; Capistrano & Chen, 2015). The loyalty of consumers to a website is tied to the level of trust they have in it. Therefore, the cultivation of trust not only impacts the intention to make purchases, as demonstrated by previous studies, but it also directly influences the actual purchasing behavior. This encompasses preferences, expenditure, visit frequency, and ultimately, the profitability derived from each consumer. Furthermore, analyses indicate that trust in the internet is notably influenced by consumers' perception of security regarding the management of their private data (Flavian & Guinaliu, 2006; Zhu and Grover, 2022). While it's recognized that current methods such as privacy policies often fail to influence consumer decision-making, there's a lack of understanding regarding the impact of alternative approaches. By examining how different presentation formats affect consumer perceptions and behaviors, researchers can identify more effective strategies for bridging the information gap between consumers and companies regarding privacy practices.

The Paradox of ‘Privacy Policy’

The "privacy paradox" refers to the inconsistency between individuals' concerns about privacy and their actual behaviors regarding privacy in the digital age. Despite expressing concerns about their privacy online, many people still willingly share personal information and engage with digital services that may compromise their privacy. This paradox highlights the complex relationship between individuals' attitudes, perceptions, and behaviors regarding privacy online (Dienlin, et al. 2021). Other studies have also indicated that most people are willing to put aside privacy concerns, providing personal information for even small rewards (Tsai et al. 2011) or because they have the believe that they are in control over their privacy choices (Shih & Liu, 2023).

Consumers generally view reading privacy notices as the primary way they manage the risks of sharing personal information with online service providers. Typically, consumers that read privacy policy are concerned for their online privacy, have positive perceptions about the notice and have higher levels of comprehension and trust in the notice (Rishab et al., 2022).

Other studies (Groom & Calo, 2021) tested through an experiment the reading behavior of online consumers. In their conclusion they stated that none of the participants in the experiment (120 in total) clicked on the policy link during engagement with a search engine. Similar studies (Obar & Oeldorf-Hirsch, 2020) reveal that 74% of the online consumers skipped reading privacy policy, selecting the ‘accept all’ without really reading it. Even in the cases that consumers read the privacy policy it lasts in average 73 seconds (when it should last 29-32 minutes). Both privacy policies and terms of service do not seem to consistently impact consumer decision making – either because the information they provide remains invisible to consumers, or because it is ignored or misinterpreted. However, the question remains: how is consumer decision-making impacted when information about a website’s privacy practices is more comprehensible and presented in an intuitive manner?

Communications of Privacy Policy

When academic researchers and industry developers design a privacy policy, they typically consider various aspects to ensure the protection of consumers personal information. Privacy policies are often filled with legal and technical language, making them difficult for the average user to fully comprehend. The new GDPR (General Data Protection Regulation) regime has increased in average the median number of sentences by 325% (Bartelt, & Buchmann, 2024). Research in the field of data visualization has extensively explored various techniques and approaches to enhance the effectiveness of visualizations in conveying information. While there is a growing recognition of the importance of privacy considerations in data handling and communication, limited attention has been directed towards integrating privacy-aware design principles into data visualization practices.

By incorporating visual aids such as icons, diagrams, infographics, and interactive features, privacy policies can become more user-friendly and engaging (Otten et al., 2015). In this context 'visual communication' encompasses a wide array of graphical design techniques can help organizations to fulfill their legal and ethical obligations to provide clear and transparent privacy information to users, ultimately enhancing user trust and compliance with data protection regulations. Adding visualizations to online agreements has been shown to capture greater attention from readers and prolong the time they spend engaging with the content, as noted by Viegas et al. (2009). Additionally, research by Harkous et al. (2018) suggests the development of an automated system called Polisis, which aims to simplify the analysis of privacy policies and the automated assignment of privacy icons from privacy policies.

The new GDPR regime support a “user-centric rather than legalistic” interpretation of the rights of consumers over their personal data control. It explains that “the quality, accessibility, and comprehensibility of the information is as important as the actual content of the transparency information” (Article 29 Data Protection Working Party, 2018), focusing on transparency-enhancing solutions that should be designed for the goals of serving different users backgrounds and with different digital literacy. Recent studies in Albania indicate that consumers are becoming more aware of data protection issues (Hasrama et al., 2024). This has led to an increase interest of companies on transparency as an opportunity to create a competitive advantage and as a mean to export their services. GDPR applies not only to organizations based within the EU but also to those outside the EU that offer goods or services to individuals in the EU or monitor their behavior. Transparency in this case should use useful techniques that clearly communicate to users how their personal information will be collected, used, stored, and shared. This includes providing information on data collection methods, purposes, and any third parties involved. While greater transparency typically correlates with improved clarity, it should also prioritize simplifying complex and vast information, emphasizing the most pertinent details, and facilitating a quick overview followed by deeper exploration into specific issues (Rossi & Lenzini, 2020).

Privacy-aware design encompasses a holistic approach to data visualization that takes into account the context, audience, and purpose of the data story while prioritizing user privacy. Despite its potential significance in safeguarding user privacy and fostering trust in data-driven environments, there remains a scarcity of empirical studies and theoretical frameworks that specifically address privacy considerations in the design and implementation of data visualizations. Several researches have stated that the way that the privacy policy is presented to the users is an important factor that affects users' privacy awareness level (Soumelidou & Tsohou, 2019; Ebbers et al., 2020; Gou et al., 2023).

Scope of the research

With the increasing prevalence of data breaches and cyber-attacks, internet users are becoming more aware of the importance of privacy. However, many users lack the knowledge and tools to effectively protect themselves. The complexity and fast development of the digital ecosystem, with numerous platforms, apps, and devices collecting and sharing user data requires a level of awareness and technical understanding that many users lack. Technology is constantly evolving, introducing new privacy threats and vulnerabilities. Despite the growing awareness of privacy issues, many users are unsure about what steps they can take to protect their personal information online. There's a need for educational resources and guidance tailored to users' specific needs and skill levels.

The introduction of privacy regulations such as GDPR and CCPA highlights the importance of privacy compliance for businesses. However, individuals also need tools to understand their rights under these regulations and how they can exercise them effectively. Every user's privacy needs and preferences are unique. A one-size-fits-all approach to privacy awareness may not be effective. Instead, there's a need for tools that can personalize recommendations and guidance based on individual circumstances. Empowering users to take control of their privacy is essential for fostering trust and confidence in the digital ecosystem.

Objective 1: To know how e-commerce websites in Albania collects and uses consumers data. The research also aims to explore the objective and subjective elements of privacy policies and to explore how these elements affect user's perception on website trust and help to enhance users' awareness on privacy policy. Additionally, the research seeks to offer recommendations for improving the accessibility and user-friendliness of privacy policies on e-commerce websites in Albania. By examining both objective elements, such as the structure and language of privacy policies, and subjective elements, such as user perceptions and trust, the study aims to provide insights into how privacy policies can be optimized to enhance user awareness, trust, and satisfaction. Ultimately, the findings of this research will contribute to the development of best practices for privacy policy design and implementation, promoting a more transparent and secure online environment for consumers in Albania.

Objective 2: The second part of the study aims to recognize the importance of privacy policy to be accepted and perceived as a tool that helps users understand how their personal data are used and secured. The privacy awareness helps users to make a decision on acceptance or rejection of privacy policies.

Hypotheses of the study

Website perception

Frik & Mittone (2019) investigated the effect of privacy assurance mechanisms, including the presence of a privacy policy, on consumer trust and behavioral intentions. They found that a privacy policy link well displayed in the website will positively influenced consumers' perceptions of the website trustworthiness, leading to greater willingness to provide personal information. Websites with clear and easily accessible privacy policies are more likely to be perceived as trustworthy by users (Bansal et al. 2015). Broeder (2020) examined the impact of privacy policy statements on users' trust in online transactions. They found a positive correlation between the presence of a privacy policy and users' trust in e-commerce websites. Websites that provided clear and comprehensive privacy policies were perceived as more trustworthy, leading to increased user confidence in conducting online transactions.

Hypothesis 1

A website with a notable privacy policy will be considered more trustworthy to interact with.

Hypothesis 2

Websites with clearly communicated and secure privacy policies will be perceived more positively by users in terms of trust and credibility compared to websites with vague privacy policies.

Privacy policy structure

Esmaeilzadeh, (2019) explores users' perceptions of privacy and self-disclosure on social networking sites. It highlights the importance of transparent privacy policies in shaping users' trust and willingness to share personal information. Bruening & Culnan (2015) findings results that long privacy notices if are presented in visual appealing format and elements can compete with other sources of information for user’s attention. Additional studies provide further insights into the complex relationship between privacy policies, user perceptions, and behaviors online. They underscore the importance of not only having privacy policies but also ensuring they are easily accessible, readable, and aligned with users' expectations to foster trust and encourage disclosure of personal information (Acquisti et al. 2017).

Hypothesis 3

A website with a visual-friendly privacy policy structure will be considered more transparent than a website with a ‘overtechnical’ privacy notice.

User data control

Mousavi et al. (2020) study investigates how user control features in privacy policies influence consumers' perceptions of online privacy. It emphasizes the importance of providing users with control over the collection, use, and sharing of their personal information to enhance trust and confidence in online platforms. The research suggests that privacy policies that offer robust data control mechanisms are more positively perceived by users and can lead to increased engagement and satisfaction. Taddei & Contena (2013) study examines the impact of privacy settings and controls on users' trust and willingness to share personal information. It finds that users who perceive greater control over their privacy settings are more likely to trust the platform and engage in self-disclosure. Furthermore, the research highlights the importance of user-friendly interfaces and clear communication of privacy controls to empower users in managing their privacy effectively.

Hypothesis 4

A privacy policy is more positively precepted if it offers more data control for users.

Anthropomorphism

The diverse literature underscores the importance of anthropomorphic design elements in shaping user perceptions, behaviors, and brand interactions across various domains, including interface design, marketing, and brand management. Böcking, Lins, and Heuten (2015) examined the role of anthropomorphic design in online services. They found that incorporating anthropomorphic elements into website design can enhance user experience and engagement, particularly in e-commerce and social networking platforms. Other studies found that anthropomorphic design elements can evoke emotional responses and influence user engagement and satisfaction with the interface (Park et al. 2015).

Hypothesis 5

The inclusion of an anthropomorphic character in a privacy policy will lead to reduced disclosure of personal information compared to privacy policies without such a character

Privacy awareness

The literature suggests that awareness of privacy policies plays a significant role in shaping users' intentions to disclose personal information online. Transparent and comprehensible privacy policies are essential for fostering trust and empowering users to make informed choices about their privacy (Chang et al. 2018; Flavián & Guinalíu, 2006). Other findings suggested that users who were more aware of privacy policies were more cautious about sharing personal information online, indicating a link between awareness and behavior (Bulgurcu et al. 2010).

Hypothesis 6

Awareness on privacy policy will be accompanied with the intention to interact with more confidence with the website.

These hypotheses are formulated based on the gaps and themes identified in the literature, aiming to contribute new insights to this field of research.

ANALYSES RESULTS

Hence, we identified and manually analyzed 9 most visited ecommerce websites in Albania according to Semrush (table 1). The main findings from the analyses of these privacy policies include accessibility to the privacy policy, structure and language, main sections, readability, personal data control, data collection, accessibility, security, and other findings. After visiting each of the websites, we identified the link to its privacy policy. Each of the privacy policy was downloaded and was manually analyzed if it included the important guidelines of the GDPR (table 3) like transparency and communication, what data is collected, users' rights for access, right to be forgotten and to restrict data processing, accountability, privacy settings and data security.

Table 1. Privacy policy used for validation

E-commerce	Privacy Policy Link
Megatek	https://www.megateksa.com/sq/privacy-policy-cookie-restriction-mode
Aladini	https://aladini.al/content/termat-dhe-kushtet.html
Gjirafa	https://gjirafa.com/Top/Terms#Privacy
MerJep.al	https://www.merrjep.com/kujdesi-ndaj-klientit/politika-e-cookies
Baboon	https://www.baboon.al/termat-kushtet#terms_of_use_14
Neptun	https://www.neptun.al/politika-e-privat-sis.nspx
TopShop	https://www.topshop.al/ruajta-e-fshehtesise/
Shpresa.al	https://shop.shpresa.al/privacy-policy/
Ecommerce Albania	https://ecommercealbania.com/

Length and complexity of privacy policies

Various research studies have indicated that a small percentage of consumers actively interact (read and understand) with privacy policies and terms and conditions when signing up for online platform (Acquisti et al. 2017). Additionally, the ease of accessing this information is crucial, with the length and format of these documents playing significant roles (Barth & De Jong, 2017). This research, reveals that the terms and conditions of platforms tend to be lengthy and dispersed across multiple locations (Table 4). Notably, Gjirafa.com has the longest among the platforms studied, totaling 4,598 words structured in 21 distinct parts.

Table 2. Overview of website terms of service and privacy/data policies[1]

	Megatek	Aladini	Gjirafa	MerJep.al	Baboon	Neptun	TopShop	Shpresa.al
Terms/policies visible on front/main page?	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Approx. length in Words	1,856 in 7 parts	249 in 1 part	4,598 in 21 parts	3,280 in 14 parts	349 in 4 parts	439 in 1 part	2,134 in 12 parts	1,046 in 12 parts
Opt-in or opt-out of cookies	No	No	Yes (only for the location)	No	No	No	Yes	Yes
Acceptance of privacy policy by default	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Accessibility of privacy policy

While it was common for privacy policy links to be located at the bottom of the homepage, some websites had chosen to include the link in the header menu or footer area for easier access. Ultimately, all the websites fulfilled the goal to ensure that users can easily find and access the privacy policy to understand how their personal information is handled by the website. This consistency across websites helps users know where to look for important legal information, enhancing usability and navigation (Vu et al. 2021). Terms of Service (ToS) are sets of rules and guidelines that users must agree to abide by in order to use a service or website. While the privacy policy focuses on how personal data is collected, used, and protected, the ToS typically cover a broader range of legal and contractual aspects of the user-provider relationship. The observation noted that while there is a difference between the privacy policy and ToS, most of the websites merged the two documents (only Megatek had a separate ToS).

[1] https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf page 199.

Structure, language, and readability

The selected privacy policy had different structures but all the contents were mostly displayed in tabular format. The privacy policy Megatek.com is represented by answering the most common questions begins with a clear introduction a commitment of securing user privacy. The policy is presented in seven parts with four question: What are your rights? How to use cookies? How we collect data? How we use the collected data? And 3 other explanatory parts among which the list of cookies that they use.

The privacy policy of Gjirafa.com was structured with header and text for each header. It is important to mention that the text was not visibly separated from the header. The 21 parts of the privacy policy made that long and nor user friendly. It is important to mention that the link of the option of cookie management was unavailable.

In the third way of privacy policy display used by Shpresa.al, the information was structured into several main sections, including changes to privacy policy, data collection, usage of personal data, communication via email, user privacy options, data security, and contact information. This organization helps users navigate the document and locate specific information.

While technical language in privacy policies can enhance precision and legal compliance, it may also present challenges for users who are not familiar with the terminology. To improve accessibility and understanding, organizations should strive to strike a balance between technical accuracy and user-friendly language, using plain language explanations or providing supplementary materials to clarify complex terms (Crawford & Schultz, 2014).

For example, Megatek has a list of cookies that they collect and what information they store.

Cookie Name	Cookie Description
FORM_KEY	Stores randomly generated key used to prevent forged requests.
PHPSESSID	Your session ID on the server.
GUEST-VIEW	Allows guests to view and edit their orders.
PERSISTENT_SHOPPING_CART	A link to information about your cart and viewing history, if you have asked for this.
STF	Information on products you have emailed to friends.
STORE	The store view or language you have selected.
USER_ALLOWED_SAVE_COOKIE	Indicates whether a customer allowed to use cookies.
MAGE-CACHE-SESSID	Facilitates caching of content on the browser to make pages load faster.
MAGE-CACHE-STORAGE	Facilitates caching of content on the browser to make pages load faster.
MAGE-CACHE-STORAGE-SECTION-INVALIDATION	Facilitates caching of content on the browser to make pages load faster.
MAGE-CACHE-TIMEOUT	Facilitates caching of content on the browser to make pages load faster.
SECTION-DATA-IDS	Facilitates caching of content on the browser to make pages load faster.
PRIVATE_CONTENT_VERSION	Facilitates caching of content on the browser to make pages load faster.
X-MAGENTO-VARY	Facilitates caching of content on the server to make pages load faster.
MAGE-TRANSLATION-FILE-VERSION	Facilitates translation of content to other languages.
MAGE-TRANSLATION-STORAGE	Facilitates translation of content to other languages.

The language used to describe the cookies collected by the website appears to be highly technical, which may not be easy for all users to understand, especially those without a background in web development or technology. While the descriptions provide detailed information about each cookie's purpose, they could be simplified for better readability and comprehension by the general audience. Reidenberg et al. (2015) suggests that to make this information easier to understand, the privacy policy should use simpler language to describe the cookies and their purposes, avoiding technical words wherever possible. Also, it could offer brief explanations with hyperlinks alongside technical terms to clarify their meaning within the context of the website's functionality and data collection practices. By using more plain language, the privacy policy can ensure that users of all levels of technical expertise can understand how their data is being collected and used by the website (Tang et al. 2021). While some legal terminology is present, in all of the studied privacy policies the efforts have been made to explain complex concepts in everyday terms. This ensures that users can understand the content without requiring specialized legal knowledge.

The use of defaults

In this study 5 from 9 websites have set defaults that primarily work in the interests of the platform. Consumers’ information is collected by default and a control to opt out of personalized ads is provided, only in 2 websites. Even if this option is available in the other websites it does not seem likely that consumers will know of its existence as it is hidden in the text.

The GDPR requires all companies operating in the EU as well as foreign companies that handle personal data of people located in the EU to have a privacy policy by design. This is part of its goal to make sure personal information is both obtained and processed fairly (Li et al. 2019). All personal data must be processed in an ethical manner. Data should be collected for predetermined reasons only, and the data must be used for these reasons alone. Data must be accurate and updated when requested. With the exception of specific circumstances, such as scientific research data, the user must be identified only for as long as needed. Privacy policy needs to be easily accessible and the websites must obtain active consent from users before collecting any of their personal data. Users must check a box when creating a profile that says they agree to having their personal information saved (Degeling et al. 2018).

PRIVACY BY DESIGN

As it is explained in the GDPR Privacy by Design (PbD, Article 25) is a framework for proactively embedding privacy protections into the design and operation of systems, products, and processes, rather than addressing privacy issues as an afterthought. Privacy by Design advocates for addressing privacy considerations from the outset of any project, product, or service. It emphasizes preventing privacy violations before they occur, rather than reacting to privacy breaches after the fact. According to Rubinstein & Good (2020) Privacy by Design encourages making privacy the default setting in systems and applications. This means that privacy protections should be automatically enabled and require users to actively opt in to data collection or sharing, rather than having to opt out. This includes implementing strong data encryption, anonymization techniques, access controls, and other privacy-enhancing technologies. Privacy by Design calls for transparency in how personal data is collected, used, and shared (Tamò-Larrieux et al. 2018). It encourages providing clear and understandable privacy notices to users, disclosing the purposes of data processing, and empowering users to exercise control over their personal information.

In the recent years, researchers have increasingly delved into the analysis, visualization, and evaluation of privacy policies. According to the GDPR every organization should consider Privacy by Design and Privacy by Default. Even though the Albanian Law[2] has specific directives for the online companies to have their privacy policies and the main sections that should be included, it is important to note that the law doesn't efficiently and precisely mention the appropriate content, language or display of privacy policies in order to protect users' privacy. As mentioned above each of the selected privacy policy was manually analyzed if it included the important guidelines of the GDPR (see table 3) like transparency and communication, what data is collected, users' rights for access, right to be forgotten and to restrict data processing, accountability, privacy settings and data security.

Table 3. Privacy aspects that are taken into considered for the privacy rating

No.	Privacy Aspect from GDPR	Description	Article
1	Transparency and communication	Service Providers should process data in "a concise, transparent, intelligible and easily accessible form, using clear and plain language'	Article 12
2	Data Collection	SP should inform users if they are collecting the data, its purpose and the kind of data they are collecting.	Articles 13 & 14
3	Rights for access	Users should have the information of the personal data of theirs that SP are processing.	Article 15

[2] Nr. 9887, "Për mbrojtjen e të dhënave personale" https://akshi.gov.al/wp-content/uploads/2019/10/Ligji-Nr.9887-dat%C3%AB-10.03.2008-P%C3%ABr-Mbrojtjen-e-t%C3%AB-Dh%C3%ABnave-Personale-i-ndryshuar.pdf

Table 3…

4	Right to be forgotten	Users can request that their data should be forgotten from the website and delete personal data when it's no longer necessary	Article 17
5	Cookies	Users may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles and identify them.	Article 30
6	Privacy settings	Organization should provide best privacy settings by default or by design or allow the users to choose which data is collected	Article 25
7	Data security & accountability	Organizations are required to take technical measures for the data security mechanisms. Also, they should be held accountable for violations and in event of a data breach, the data subject has the right to get notification	Article 32, 33 & 34

Transparency and communication

Transparency and communication are essential aspects of privacy policies, ensuring that individuals have clear information about how their personal data is processed, in order to build trust with users and demonstrate compliance with GDPR requirements for informing individuals about the processing of their personal data. For example, Spotify clearly explains what data they collect, why they collect it, and how it's used. They detail how they collect information like your music preferences, device information, and location data to personalize your experience and improve their service. Spotify provides clear opt-out mechanisms and explains how users can control their privacy settings. They also outline users' rights under GDPR, such as the right to access their data, rectify inaccuracies, and delete their account if desired.

Also, Google privacy policy is comprehensive and transparent, covering a wide range of services and data processing activities. Google provides a detailed breakdown of the types of data they collect, including user-provided information, device information, and usage data. They explain how this data is used for various purposes, such as delivering personalized content, improving their services, and serving targeted ads. Google offers clear explanations of users' privacy choices and controls, such as opting out of personalized ads or managing ad settings. They also provide links to additional resources where users can learn more about their privacy options and how Google protects their data. The analysis on the selected websites indicates that only 60% of websites explicitly state their aim to provide security and privacy to users' or customers' data at the beginning of their privacy documents. This finding suggests that while some websites prioritize transparency and clarity regarding data protection objectives, to build user trust and comply with best practices in data management.

Data collection and the rights for access

Through the analyses of the websites, we identified which personal and other attributes were collected.

Table 4. Data collection from the websites

Website	Personal Information	Login Information	Cookies & Tracking Technologies	Search Data	Location Data	Payment Information	Communication Data	Social Media Data	Third Party Data
Megatek	✓	✓	✓	✓	✓	✓	✓		✓
Aladini	✓	✓	✓	✓	✓	✓	✓		
Gjirafa	✓	✓	✓			✓			✓
MerrJep	✓	✓	✓					✓	
Baboon	✓				✓		✓		
Neptun	✓		✓	✓					
TopShop	✓	✓	✓	✓					
Shpresa.al	✓		✓			✓			
Ecommerce Albania	✓	✓	✓	✓		✓	✓		

Only two of the policies mention the third-party data collection and only one of them provide some information about behavioral tracking mechanisms, including the fact that users can opt-out of cookies (Gjirafa.com states that user could request to remove the cookies at a link, but it didn't work). While 45 % of the websites mentions how the collected data will be used, the other websites don't explicitly mention the how these collected data will be used.

Right to be forgotten

Implementing mechanisms to facilitate the withdrawal of consent and the deletion of data is not only a legal requirement under regulations like GDPR, but it's also essential for maintaining trust and respecting individuals' privacy rights. It involves having robust systems in place to manage data throughout its lifecycle, including clear procedures for data deletion upon request. All of the websites request the users to send an email if they want to change or delete their personal data. Companies do not mention what mechanisms do they use to handle deletion requests and if they are properly working.

Cookies

Cookies are small pieces of data stored on a user's device by websites they visit. These cookies serve various purposes, including remembering user preferences, tracking user interactions, and enabling certain website functionalities (Degeling et al. 2018). However, they can also be used for tracking user behavior across different websites, which raises privacy concerns. GDPR has strict requirements on the use of cookies and other tracking technologies. These requirements include obtaining explicit consent from users before setting non-essential cookies, providing clear information about the types of cookies used and their purposes, and giving users control over their cookie preferences (Giese & Stabauer, 2022). This means that businesses must have mechanisms in place to allow users to exercise their rights regarding their personal data collected through cookies. Even if a website is not currently using cookies, it's still important to have a cookie policy in place. This is because the website's goals and marketing strategies may change over time, leading to the implementation of cookies or other tracking technologies. According to GDPR a comprehensive cookie policy should clearly state:

- ✓ The types of cookies used
- ✓ Purpose for which cookies are used
- ✓ Consent mechanism and managing cookie preferences.
- ✓ Specify how long data collected through cookies will be retained
- ✓ User rights regarding their personal data collected through cookies, including the right to access, amend, or delete their data.

Almost every service provider analyzed (8 out of 9) uses cookies; however, the analysis was further carried to know the cookie types and consent.

What is Cookie Consent?

Cookie consent is obtaining permission from a website visitor to store or retrieve information on their devices, such as a computer or smartphone. This information is typically used to personalize the user’s experience by providing tailored content or ads. Most websites will use some form of cookies, and most web browsers are set to accept them by default. Session cookies are considered strictly necessary cookies. Hence, per most data regulations, such as the GDPR, websites do not need to gain users' consent to set them on their devices. However, it is considered good practice to inform the users that such types of cookies are being used via either the cookie policy, privacy policy, or a general cookie consent banner. Besides being required by law, obtaining cookie consent is an excellent way to build trust with users. If you’re transparent about what cookies are being used and why people are more likely to trust your website and give their consent. Finally, getting cookie consent can help you avoid potential legal problems. Under GDPR, cookies are considered personal data because they can be used to track and identify individuals. As a result, websites that use cookies must obtain consent from visitors before setting or accessing cookies on their devices. Visitors can then choose to accept or reject the use of cookies.

Table 5: Types of cookies identified in the privacy policy analysis

Session cookie	These cookies are temporary and are deleted from the user's device when they close their web browser. Session cookies are typically used to maintain a user's session and carry out essential functions such as enabling secure login.
Persistent cookie	They are used to remember user preferences and settings across multiple visits to a website. Persistent cookies can be set to expire after a specific period or remain on the device until manually deleted by the user.
First-party cookie	These are often used to collect information about how users interact with the website. These cookies can help improve website performance and user experience.
Third-party cookie	They are commonly used for tracking user behavior across different websites and for serving targeted advertisements. Third-party cookies can raise privacy concerns because they allow third-party entities, to collect data about users' browsing habits.
Functional cookie	These cookies are used to enhance the functionality of a website and enable features such as personalization and language preferences. Functional cookies do not track users' browsing activity for marketing purposes.
Performance cookie	Performance cookies helps website owners analyze and improve user performance of their site.
Analytics cookie	Analytics cookies provide insights into website traffic, user demographics, and user behavior, which can inform marketing strategies and website optimizations.
Advertising cookie	Advertising cookies track users across different websites and create profiles to serve personalized ads. This type of cookie is often associated with third-party advertising networks.

To analyze Cookie, consent Enzuzo, a free website privacy policy checker was used.[3] Each url address of the websites was checked and according to Enzuzo results none of these websites was displaying a cookie banner to obtain consent. After examining cookies and security measures, the analysis focus was to data sharing and its utilization. It was found that

[3] https://enzuzo.com/privacy-compliance-scanner/

the majority of websites offer general statements regarding the reasons for collecting information, such as improving services, enhancing user experience, measuring consumer interest, advertising or research. However, there was a lack of a clear definition of each specific purpose for the collected information, where 55% of the websites mention third-party advertisement, and 60% of the policies, either explicitly stated or implicated that they will share user data with third parties

Privacy settings

Findings indicate that current implementations of "notice and choice" fail to provide notice or respect choice. Companies are required to provide clear and understandable information on privacy settings. In this analysis none of the website policies mention the Do Not Track signal. However, despite efforts to improve transparency, many online services still fail to provide comprehensive and user-friendly policies. Regarding opt-out mechanisms, the GDPR requires companies to offer users the ability to opt out of certain types of data processing, such as targeted advertising or sharing personal data with third parties. The analyzed online services didn’t provide visible opt-out options. The process to exercise these rights should not be complex or difficult to access as matter of design choices.

The analyzed websites provided only one email address and contact number for all the for the consumer support. Providing clear contact details allows users to reach out to the company if they have questions or concerns about their data. Without this information, users may struggle to get in touch with the appropriate party to address their privacy-related issues. Furthermore, even when contact information is provided, it might not be easily accessible or prominently displayed within the privacy policy or on the website.

Data security

Analyzing the privacy policies examples, all of the service providers mention that they value and provide data security. But they don’t mention that in case of data leak they will inform the users or what technical measures and standards are providing for data security. However, only 33% of service providers have precisely declared that collected users' data would be secured by means of encryption techniques like SSL. The security of personal information is vital for upholding individual rights, fostering trust and confidence, preventing harm, complying with legal requirements, maintaining business reputation, and fulfilling ethical responsibilities (Taherdoost, 2023).

The study also checked service providers who used ISO 27701. None of them use this international standard. ISO 27701 is a data privacy standard based on ISO 27001, the internationally recognized standard for information security management. Certification and compliance with standards, besides being a requirement of the EU, create opportunities for growth for ecommerce websites (EU4Digital, eCommerce report). The use of ISO 27701 standards directly impacts the development of businesses with international standards, promoting the increase of information security and competitiveness of businesses in both domestic and foreign markets, bringing our companies closer to the European market. For ecommerce websites, compliance with ISO 27701 means implementing robust data privacy and security measures, which are essential for maintaining trust with customers and partners. It ensures that personal data collected and processed through ecommerce platforms is handled securely and in accordance with international best practices, thereby reducing the risk of data breaches and enhancing the reputation of the ecommerce business.

METHODOLOGY OF THE EXPERIMENT

Participants will consist of two groups of students, both bachelor and master programs recruited from the university, N=90. Each group will comprise an equal number of participants to ensure balanced representation. Informed consent will be obtained from all participants. The experiment will be conducted following ethical guidelines and regulations of the university.

Experimental Design

The experiment will utilize a between-subjects design, where participants will be randomly assigned to one of two groups. One group will be presented with a privacy policy rated highest in the initial part of the study, while the other will be presented with a privacy policy rated lowest. These ratings were determined based on evaluations conducted in the earlier phase of the study, where the websites' privacy policies were examined and assessed. Each group was presented with the respective privacy policy on a computer. Participants were instructed to carefully read the privacy policy provided to them. After reading the privacy policy, participants completed a survey questionnaire assessing their awareness of privacy practices, including questions related to transparency, trust, security, and control over personal data. All items were adapted from validated measures.

A Mann-Whitney U test was conducted to compare the overall privacy awareness scores between the two groups and whether there is a significant difference between the medians of the two independent groups. After visiting the websites and reading the privacy policies of each of the websites participants were invited to answer a questionnaire structured in four parts. The first section of the questionnaire requested some basic sociodemographic information of participants in terms of gender (52.3% were male, 47.7% were female) and age (45.0% less than 20 years old, 55% were between 20 and 35 years old).

The second part of the questionnaire consisted on 27 questions (Appendix A) to measure participants general perceptions and intentions towards the website, using items of transparency (Bruening & Culnan, 2015), trust and security perceptions of an e-commerce website The third part of the questionnaire measured the privacy policy effectiveness like length and structure of the text based on (Frik & Mittone (2019). The third part of the questionnaire consisted of measures about users' experience toward the privacy policy and included scales of data control (Mousavi et al. 2020), awareness and intention to accept the privacy policy (based on Chang et al. 2018), and the perception if the website policy respects their personal privacy. All the items in the measurement instrument were based on 5-point Likert scales. These scales provided Cronbach alpha values between 0.91 and 0.97, above the 0.8 threshold recommended value (Taber, 2018).

Table 6. Privacy policy perception results of the exploratory replication study

Category	Variable	Experimental conditions		t-value
		Highest rated privacy policy	Lowest rated privacy policy	
Website related perceptions of intrusiveness	Transparency	2.73	2.93	-0.51
	Trust	2.62	2.80	-0.54
	Security	2.72	3.06	-0.90
Privacy policy effectiveness	Length	2.01	2.58	-1.75*
	Structure	0.58	0.40	-1.15*
Privacy policy related perceptions and intentions	Data control	4.66	2.86	4.28***
	Awareness on privacy policy	4.76	3.46	2.42**
	Intention to accept the privacy policy	4.38	2.52	3.85***

Notes: * p<0.10, ** p<0.05, *** p<0.01

A manipulation check was employed to assess the effectiveness of the privacy policy cues at the beginning of the experiment. The manipulation was found to be effective across the two groups. Those in the highest rated privacy policy condition exhibited elevated levels of online trust (M =.96, SD = .42) compared to those in the lowest rated privacy policy condition which expressed decreased levels of online trust (M = .65, SD = .40). These observed differences in levels of online trust between the two groups were highly significant, F (2, 1178) =

34.98, p < .001, η 2 = .06, attesting to internal validity of the experimental treatments. Results confirmed that the highest rated privacy presented a lower level of perceived intrusiveness than the lowest rated privacy (M = 4.09, M = 2.03; t (76) = 4.32, p < 0.01).

The highest rated privacy policy condition led to increased participant awareness of privacy practices among websites. A Mann-Whitney U test, was performed and the results found that participants who read this privacy policy on overall had higher privacy awareness (M=11.9, SD= 6.77) than the second group of the experiment (M=8.95, SD=6.75), with U (1,290)=-2.92, p=.001, r=.172). Also, using this test, results shown that women (Mean= 12.14, SD=5.89) had higher overall privacy practice awareness than men (Mean=9.85, SD=7.14), with (H (1,453) =-2.017, p=.030, r=.112).

Based on the data, transparency, trust, and security perceptions did not differ significantly between the two privacy policy conditions. The t-values for length and structure indicate that there are statistically significant differences between the highest and lowest rated privacy policy conditions. Specifically, websites with the highest rated privacy policies were perceived to have more effective privacy policies in terms of length and structure compared to those with the lowest rated privacy policies. According to privacy policy related perceptions and intentions (data control, awareness on privacy policy, intention to accept the privacy policy), the t-values for these variables indicate that there are statistically significant differences between the highest and lowest rated privacy policy conditions. Specifically, websites with the highest rated privacy policies were associated with higher levels of data control, awareness of the privacy policy, and intention to accept the privacy policy compared to those with the lowest rated privacy policies.

These findings highlight the importance of clear and high-quality privacy policies in enhancing users' awareness of privacy practices on websites. Additionally, they suggest the need for further exploration of gender differences in privacy awareness and the potential nuances in how individuals process privacy-related information. However, the lack of significant interaction between notice length and privacy awareness to further investigate the factors influencing users' comprehension of privacy practices online.

CONCLUSION

The extensive analysis of privacy policies and the experimental study conducted offers some important insights on the role of clear and user-friendly privacy policies in shaping users' awareness and perceptions of privacy practices on websites. These findings align with previous research, which has consistently highlighted the importance of transparent and accessible privacy policies in building trust and empowering users to make informed decisions regarding their personal data (Barth & De Jong, 2017; Acquisti et al., 2017; Vu et al., 2021).

Length and complexity emerged as critical factors impacting user engagement and understanding of privacy policies. Therefore, it is imperative for websites to strive for simplicity and clarity in their privacy policy language, ensuring that technical terms are explained in plain language to accommodate users of varying technical expertise (Crawford & Schultz, 2014). Additionally, providing supplementary materials or hyperlinks to further explanations can enhance users' comprehension and foster transparency. Despite regulatory requirements such as GDPR mandating user consent for data collection, the analysis revealed that many websites default to data collection without clear opt-out mechanisms, potentially undermining user privacy (Li et al., 2019). It is imperative for websites to prioritize user interests by offering transparent options for opting out of data collection or personalized ads, thereby respecting users' privacy preferences and rights. Furthermore, the implementation of Privacy by Design principles emerged as a promising approach to embed privacy protections into website design and operations. By proactively integrating privacy considerations, websites can enhance user trust and compliance with regulatory frameworks such as GDPR (Rubinstein & Good, 2020). This aligns with the growing recognition of Privacy by Design as a foundational framework for promoting privacy and data protection in digital ecosystems.

The experimental study underscored the positive impact of high-quality privacy policies on users' awareness, trust, and perceptions of website privacy practices. This corroborates with previous research emphasizing the importance of clear, concise, and well-structured privacy policies in enhancing user engagement (Frik & Mittone, 2019) and foster a safer and more trustworthy online environment. The observation of potential gender differences in privacy awareness suggests the need for further exploration into how different demographics process privacy-related information. Understanding these nuances can inform tailored privacy communication strategies to effectively engage diverse user groups and promote privacy literacy across various segments of the population.

In conclusion, the findings highlight the importance of user-friendly privacy policies to enhance transparency, trust, and user empowerment in the digital age. Future research should continue to explore innovative approaches to privacy communication and examine the impact of demographic factors on privacy awareness and perceptions. By advancing our understanding of privacy practices, we can achieve a more informed online ecosystem for all users.

REFERENCES

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users’ choices online. ACM Computing Surveys (CSUR), 50(3), 1-41.

Ackermann, K., Miesler, L., Mildenberger, Th., Frey, M., Bearth, A. (2021). Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. Journal of Consumer Behaviour. 21. 10.1002/cb.2012.

Bartelt, B. & Buchmann, E. (2024). Transparency in Privacy Policies. Twelfth International Conference on Building and Exploring Web Based Environments.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and informatics, 34(7), 1038-1058.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. European Journal of Information Systems, 24, 624-644.

Böcking, S., Lins, J., & Heuten, W. (2015). Anthropomorphic design in online services. In Proceedings of the 2015 British HCI Conference (pp. 286-287).

Bonneau, Joseph & Preibusch, Sören. (2010). The Privacy Jungle:On the Market for Data Protection in Social Networks. 10.1007/978-1-4419-6967-5_8.

Broeder, P. (2020). Culture, privacy, and trust in e-commerce. Marketing from Information to Decision Journal, 3(1), 14-26.

Bruening, P. J., & Culnan, M. J. (2015). Through a glass darkly: From privacy notices to effective transparency. NCJL & Tech., 17, 515.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 523-548.

Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. Computer Standards & Interfaces, 42, 24-31.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers’ perceived privacy. Government Information Quarterly, 35(3), 445-459.

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. BCL Rev., 55, 93.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. arXiv preprint arXiv:1808.05096.

Dienlin, T. & Masur, P. K. & Trepte, S. (2021). A longitudinal analysis of the privacy paradox. New Media & Society. 25. 146144482110163. 10.1177/14614448211016316.

Ebbers, F., Zibuschka, J., Zimmermann, C., & Hinz, O. (2020). User preferences for privacy features in digital assistants. Electronic Markets, 31, 411 - 426.

Esmaeilzadeh, P. (2019). The impacts of the perceived transparency of privacy policies and trust in providers for building trust in health information exchange: empirical study. JMIR medical informatics, 7(4), e14050.

Flavian, C & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. Industrial Management and Data Systems. 106. 601-620. 10.1108/02635570610666403.

Frik, A., & Mittone, L. (2019). Factors influencing the perception of website privacy trustworthiness and users’ purchasing intentions: The behavioral economics perspective. Journal of theoretical and applied electronic commerce research, 14(3), 89-125.

Giese, J., & Stabauer, M. (2022). Factors that influence cookie acceptance: Characteristics of cookie notices that users perceive to affect their decisions. In International Conference on Human-Computer Interaction (pp. 272-285). Cham: Springer International Publishing.

Guo, Y., Liu, F., Zhou, T., Cai, Z., & Xiao, N. (2023). Seeing is believing: Towards interactive visual exploration of data privacy in federated learning. Inf. Process. Manag., 60, 103162.

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., & Aberer, K. (2018). Polisis: Automated analysis and presentation of privacy policies using deep learning. In 27th USENIX Security Symposium (USENIX Security 18) (pp. 531-548).

Hasrama, E & Myftaraj, E & Trebicka, B. (2024). Exploring User Attitudes Toward Online Behavioral Advertising: Insights into Trust, Transparency and Privacy. Academic Journal of Interdisciplinary Studies. 13. 380. 10.36941/ajis-2024-0054.

Kröger, J. L., Lutz, O. H. M., & Ullrich, S. (2021). The myth of individual control: Mapping the limitations of privacy self-management. Available at SSRN 3881776.

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. Journal of Global Information Technology Management, 22(1), 1-6.

Obar, J. A. & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, Information, Communication & Society, 23:1, 128-147, DOI: 10.1080/1369118X.2018.1486870

Otten, J., Cheng, K. & Drewnowski, A. (2015). Infographics and Public Policy: Using Data Visualization To Convey Complex Information. Health Affairs. 34. 1901-1907. 10.1377/hlthaff.2015.0642.

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decision Support Systems, 135, 113323.

Park, B., Knörzer, L., Plass, J. L., & Brünken, R. (2015). Emotional design and positive emotions in multimedia learning: An eyetracking study on the use of anthropomorphisms. Computers & Education, 86, 30-42.

Ravichander, A., Black, A., Norton, T., Wilson, S., & Sadeh, N. (2021). Breaking down walls of text: How can nlp benefit consumer privacy? In ACL.

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., ... & Schaub, F. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Tech. LJ, 30, 39.

Rishab B., Smriti P., Faiza R. & Renuka S., (2022). Disclosures in Privacy Policies: Does "Notice and Consent" Work?, 33 Loy. Consumer L. Rev. 1, https://lawecommons.luc.edu/lclr/vol33/iss1/5

Rubinstein, I. S., & Good, N. (2020). The trouble with Article 25 (and how to fix it): the future of data protection by design and default. International Data Privacy Law, 10(1), 37-56.

Rossi, A. & Lenzini, G., (2020). Transparency by design in data-informed research: A collection of information design patterns, Computer Law & Security Review, Volume 37, 105402, https://doi.org/10.1016/j.clsr.2020.105402

Soumelidou, A., & Tsohou, A. (2019). Effects of privacy policy visualization on users' information privacy awareness level. Inf. Technol. People, 33, 502-534.

Steinfeld, N. (2016). “I agree to the terms and conditions”(How) do users read privacy policies online? An eye-tracking experiment. Computers in human behavior, 55, 992-1000.

Spiekermann, Sarah and Berendt, Bettina and Grossklags, Jens, E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. CACM, Vol. 48, No. 3, 2005, Available at SSRN: https://ssrn.com/abstract=761107

Shih, HP., Liu, W. (2023). Beyond the trade-offs on Facebook: the underlying mechanisms of privacy choices. Inf Syst E-Bus Manage 21, 353–387 https://doi.org/10.1007/s10257-023-00622-6.

Taber, K. S. (2018). The use of Cronbach’s alpha when developing and reporting research instruments in science education. Research in science education, 48, 1273-1296.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure?. Computers in human behavior, 29(3), 821-826.

Tabassum, M., Alqhatani, A., Aldossari, M., & Lipford, H. R. (2018). “Increasing user attention with a comic-based policy”. in Proc. CHI Conf. Hum. Factors Comput. Syst., Apr. 2018, pp. 1–6.

Tang, J., Shoemaker, H., Lerner, A., & Birrell, E. (2021). Defining privacy: How users interpret technical terms in privacy policies. Proceedings on Privacy Enhancing Technologies.

Tamò-Larrieux, A., Tamò-Larrieux, S., & Seyfried. (2018). Designing for privacy and its legal framework.

Taherdoost, H. (2023). Legal, Regulatory, and Ethical Considerations in E-Business. In E-Business Essentials: Building a Successful Online Enterprise (pp. 379-402). Cham: Springer Nature Switzerland.

Tesfay, W, & Hofmann, P, & Nakamura, T, & Kiyomoto, Sh. & Serna, J. (2018). Privacy Guide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation. 15-21. 10.1145/3180445.3180447.

Tsai, J., Cranor, L., Acquisti, A., Fong, C., (2007). What's It To You? A Survey of Online Privacy Concerns and Risks. NET Institute Working Paper No. 06-29.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research, 22(2), 254–268. http://www.jstor.org/stable/23015560

Viegas, F. B., Wattenberg, M., & Feinberg, J. (2009). Participatory visualization with wordle. IEEE transactions on visualization and computer graphics, 15(6), 1137-1144.

Vu, K. P. L., Proctor, R. W., & Hung, Y. H. (2021). Website design and evaluation. Handbook of human factors and ergonomics, 1016-1036.

Zhu, Y., Grover, V. (2022). Privacy in the sharing economy: Why don't users disclose their negative experiences?, International Journal of Information Management, V 67, 102543, https://doi.org/10.1016/j.ijinfomgt.2022.102543