Dissecting Privacy Perspectives of Websites Around the World: "Aceptar Todo, Alle Akzeptieren, Accept All..."

Aysun Ogut, Berke Turanlioglu, Doruk Can Metiner, Albert Levi, Cemal Yilmaz, and Orcun Cetin, *Sabanci University, Tuzla, Istanbul, Turkiye;* Selcuk Uluagac, *Cyber-Physical Systems Security Lab, Florida International University, Miami, Florida, USA*

https://www.usenix.org/conference/usenixsecurity24/presentation/ogut

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Proceedings of the 33rd USENIX Security Symposium is sponsored by USENIX.

Dissecting Privacy Perspectives of Websites Around the World: "Aceptar Todo, Alle Akzeptieren, Accept All..."

Aysun Ogut[1], Berke Turanlioglu[1], Doruk Can Metiner[1], Albert Levi[1], Cemal Yilmaz[1], Orcun Cetin[1], and Selcuk Uluagac[2]

[1]Sabanci University, Tuzla, Istanbul, Turkiye
[2]Cyber-Physical Systems Security Lab, Florida International University, Miami, Florida, USA
{aysuno, berket, dorukmetiner, levi, cyilmaz, orcun.cetin}@sabanciuniv.edu, selcuk@cs.fiu.edu

Abstract

Privacy has become a significant concern as the processing, storage, and sharing of collected data expands. In order to take precautions against this increasing issue, countries and different government entities have enacted laws for the protection of privacy, and articles regarding acquiring consent from the user to collect data (i.e., via cookies) have been regulated such as the right of one to be informed and to manage their preferences. Even though there are many regulations, still many websites do not transparently provide their users with their privacy practices and cookie consent notices, and restrict one's rights or make it difficult to set/choose their privacy preferences. The main objective of this study is to analyze whether websites from around the world inform their users about the collection of their data and to identify how easy or difficult for users to set their privacy preferences in practice. While observing the differences between countries, we also aim to examine whether there is an effect of geographical location on privacy approaches and whether the applications and interpretations of countries that follow and comply with the same laws are similar. For this purpose, we have developed an automated tool to scan the privacy notices on the 500 most popular websites in different countries around the world. Our extensive analysis indicates that in some countries users are rarely informed and even in countries with high cookie consent notifications, offering the option to refuse is still very low despite the fact that it is part of their regulations. The highest rate of reject buttons on cookie banners in the countries studied is 35%. Overall, although the law gives the user the right to refuse consent and be informed, we have concluded that this does not apply in practice in most countries. Moreover, in many cases, the implementations are convoluted and not user-friendly at all.

1 Introduction

Just as you do not immediately accept and reply to an email requesting your private information, do you respond in a similar manner when a website asks for your data? Websites collect *cookies* (i.e., save information) from their users to reason about how they behave and operate while browsing their platforms. Although it is stated in privacy notices and policies that the data is collected for session continuity and functionality, most of the user cookies supply data for advertising purposes [8] to third parties [26]. Therefore, the background flow and record-keeping of cookies have fueled advertising and marketing initiatives in online environments all over the world [3, 9]. User-targeting data is highly valuable for service providers to optimize the services accordingly. Consequently, data privacy has become an inevitable issue when it comes to the massive transfer of data.

Privacy and its violations are significant concerns that draw the attention of consumers through occasional scandalous news such as Facebook sharing user information with Cambridge Analytica [4, 27, 41] and Meta/WhatsApp introducing a controversial privacy policy [14, 42]. Experiencing such circumstances has led individuals and regulators to gain awareness and take the necessary steps to protect users' privacy. One of the actions taken is the development of consent notices that inform users about the collection of cookies and ask for their explicit permissions for privacy. These cookie consent notices are usually placed at the top of the website interface and may consist of parts such as text informing the user about cookie collection, accepting, rejecting, and editing preferences, and a closing icon via buttons. Figure 1 shows the set of accept example buttons that we came across during our study. While some regulations, such as GDPR [17], legally declare that the user's explicit approval is mandatory, it has been repeatedly observed that websites do not comply with these rules all the time [10, 34]. This raises the question of whether the user is truly safe and aware of their rights on the Internet.

To the best of our knowledge, our study is the first empirical study in the literature to investigate and compare privacy notifications of various countries globally in terms of depth to reach the reject option, size classification, and complexity of the text. To this end, we analyzed 500 websites from each subject country selected for the study: Brazil, Bulgaria, Germany,

Figure 1: Example buttons on banners we encountered during the study.

Italy, Japan, Russia, Turkiye, and the United Kingdom. During our investigation in these countries, we established remote (from Turkiye and the US) and local connections to observe the attitudes towards both internal and external users. Our work helps to comprehend whether (i) user-centered privacy perspectives of the websites vary across countries, (ii) the geographical location affects the application or interpretation of privacy, (iii) there is a distinction in the implementation of the privacy regulations adhering to the same privacy laws.

The results of our extensive analysis indicate that the display of the cookie consent notices for countries enforcing strict privacy regulations, such as European countries, was 64%, compared to those countries having loose regulations, and/or regulations are not enforced, such as Russia with 28% and Japan with 8%. Granting users the right to refuse consent, Germany ranks first with 35%.

Due to world-renowned news on privacy violations and sharing extensive user data with third parties without getting consent, many studies on online privacy practices and the extent of the collected data have been published before. Indeed, previous studies have found that not every website that collects cookies informs its users about this issue and does not obtain their permission. They found that the majority of websites do not display cookie banners on their sites [10, 30, 34]. Nevertheless, most of the existing research on the topic is GDPR-centric, evaluating European websites and compliance with GDPR. Therefore, the literature lacks worldwide research presenting comparative statistics and evaluating the practices on multiple metrics.

Contributions: Our study reveals a broader domain of research by;

- Investigating the most popular websites located in different countries around the world for their privacy practices.
- Creating a tool to automatically check privacy notices via cookie consent banners, along with the layout, text analysis, and clickable options provided. Our tool has revealed that only 37.7% of all the websites (24% for the countries analyzed from the US) investigated within the scope of the research have a cookie consent banner.
- Analyzing the depth of rejecting the privacy policy. It has been observed that users can reject the privacy policy with a single click for only 21.9% of websites with a cookie consent banner for the country with the best statistics.
- Providing insights on the complexity of the text on the cookie consent banner, classification of the banner according to the ratio of web page sizes, and whether a privacy policy redirect is added in the footer of the website.

Organization: The remainder of this paper is organized as follows: Section 2 provides background information by briefing the results of the related previous studies. Section 3 describes the privacy practices of the studied countries and the details about the means of the investigation. Section 4 presents all the findings and comparisons of privacy notices of the countries. Section 5 discusses the inferences between all the data obtained and the research questions, and the meaning of the data. Finally, Section 6 concludes the paper.

2 Related Work

There have been studies conducted on user-centric privacy policies and data privacy regulations followed by countries. While most of the earlier research is done on European countries and GDPR, there have been several explorations on developing tools to quantify the privacy level on individual websites as well.

Degeling et al. [10] investigated the effect of GDPR on the privacy practices on the websites of European countries. As an outcome of the study conducted on 500 websites from each European country, they identified a positive effect on user-centric privacy practices. To explain user-centric privacy practices, it can be said that all kinds of texts, banners, and menu items provided to the users, as well as the options proposed as a part of these visualizations, are considered user-centric privacy practices. As an outcome of the work conducted by Degeling et al., statistically speaking, the number of cookie consent notices increased from 46.1% to 63.2% across Europe after GDPR came into effect. Kretschmer et al. [24] also identified a similar impact of GDPR on privacy practices. According to their study, the amount of third-party tracking on the web revealed a decrease with an increase in user-centered privacy practices, such as providing a cookie consent notice with options to the users.

Kokciyan and Yolum [21] have developed a web-based tool that identifies privacy violations based on the comparison of consent taken from the user and what is collected. They have identified that as the size of the social network of a user increases, the violations, thus the amount of time required to identify these violations, also increases. Their work suggests a complex network full of interaction between parties for the medium of exchange of user-generated data.

Taking another aspect of the topic as the central concern, Dotras and Ros [23] investigated the compliance of websites from different countries with GDPR for processing the data of their European customers. They identified that, even within Europe, differences exist between a country being a main domain versus a subdomain. Compliance with GDPR was higher when the connection was constructed from the main domain. Looking at cookie consents from a more global perspective, Sanchez-Rola et al. [29] examined websites in the US and EU to understand the effect of GDPR. They observed almost identical website behavior in the results obtained from within and outside Europe. The results show that 92% of the websites track the user without notifying them. When it comes to giving users an opt-out option, they found that only 4% did so.

Santos et al. [30] and Utz et al. [40] proposed work on the cookie consent notices themselves by investigating the banners presented to the users. They identified ambiguous expressions in almost half of the displayed cookie notices despite 60% of notices declaring that cookies are being used *to improve user experience*. Trevisan et al. [22] conducted similar research and statistically presented the privacy compliance of the cookie notices in Europe to the regulations. Their findings also indicate that 49% of the websites do not comply with the regulations in effect. Carpineto et al. [7] performed this check within a smaller domain, namely the websites in Italy, and concluded that institutional websites are ahead of commercial ones at complying with the regulations. Similarly, Nouwens et al. [25] investigated the compliance of cookie consent notices with regulations on UK websites. They found that only 11.8% of websites displayed legal designs and the presence or absence of elements such as an opt-out button in these designs affects the consent rate.

Differences From Existing Work: We extend the scope of the research to a worldwide domain instead of focusing on GDPR and the European Union. Therefore, a user can know how their data is treated worldwide. Previous studies in this field have been conducted with a smaller set of countries. Along with the extension, we collect key factors such as banner and text evaluation, footer existence, and layout providing insights into the privacy perspectives of the websites to extract valuable information from them and address a wider aspect of a website while evaluating the results. Moreover, by highlighting the contrasts of varying geographical zones, we present statistical data from a selection of countries in different locations.

3 Objectives and Methodology

The main objective of our research is to study the user-centric privacy perspectives of websites between countries by analyzing privacy notices via cookies. To deepen the understanding of privacy notices, we provide a brief introduction to cookies and their purposes.

Cookies: Cookies are data files kept on the hard drive of the device they're being collected on, which store information about both the user and the visit performed. [16] The information collected ranges from time spent on the website to items added to the shopping cart. Websites themselves collect cookies from their visitors to gain insights about their visitors and also to sell these data to third parties. In a wider scope, cookies become an important data source that shapes the marketing and advertising sector [2, 8] and has significant value. In light of the information provided about cookies, privacy notices enlighten users about the content of cookies placed by the website and the parties they are shared with and ask for consent.

The following research questions (RQ) constitute our main scope for this work:

RQ1: *How do the user-centered privacy perspectives of websites differ across countries globally?*

RQ2: *To what extent does geographical location influence the privacy-related practices adopted by countries?*

RQ3: *How similar are cookie consent notices in countries that adhere to the same data protection regulations?*

With all these research questions in mind, we pick the countries in accordance with the cultural zones they belong to (see Figure 2) with a restriction of being a G20 country or being in a union that is part of G20. We aimed to direct the research conducted to relatively larger economies where both domestic and international companies are effective. We believe that more variance in the content of websites will help us get the opportunity to analyze the internalization of privacy policies by all segments of the population. Furthermore,

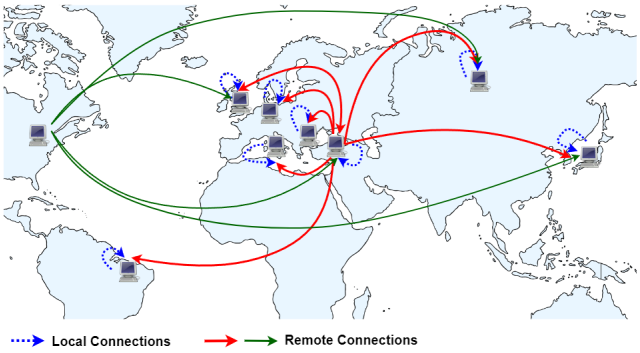


Figure 2: Countries involved: Brazil, Bulgaria, Germany, Italy, Japan, Russia, Turkiye, UK, and and US. The red and green lines represent the remote connections and the blue line represents the local connections. Two differently colored remote connections display different established links in the study.

while selecting amongst the larger economies, we gave priority to countries where comparison with each other would give meaningful results and countries with greater interest. As a result, we opted to pick Brazil, Bulgaria, Germany, Italy, Japan, Russia, Turkiye, the UK, and the US (as a consistent third country).

3.1 Subject Countries and Their Privacy Legislations

In order to draw meaningful results, it is important to understand the countries' perspectives on privacy and the privacy regulations they are currently adopting. This section describes the recent data protection laws of the countries.

Brazil: In 2018, the General Personal Data Protection Law (LGPD), enacted by The Brazilian Federal Constitution, has effectively ensured the security of individuals on the Internet. Consisting of 65 articles, this law offers similarities with the GDPR published by the European Union [5].

Bulgaria: Bulgaria, which has been included in the European Union since 2007, has a guideline for data protection named the Commission for Personal Data Protection (CPDP) along with adopting the GDPR provisions. It does not demonstrate major differences and some legal bases such as consent, legal obligations, and contract with the subject directly adopt the GDPR regulations [6].

Germany: Germany was one of the first EU member countries to adopt the GDPR. The Federal Data Protection Act (BDSG), working alongside the GDPR, has been effective in 2017, and states the limitations and rights of users and data collectors. The BDSG also includes laws on data transfers and cookie consents [13].

Italy: Italian Personal Data Protection Law (The Code) was replaced by GDPR in 2018, and The Italian Data Protection Authority (Garante) is competent in the enforcement of the personal privacy regulations [18]. Some articles in The Code directly contradicted GDPR [19].

Japan: The Act on the Protection of Personal Information (APPI) regulations were effective in 2017 and later with revisions in 2022. While it is mentioned that data protection is one of the most active areas of Japanese law, there is an article that it is mandatory to acquire consent before obtaining data from the user [20].

Russia: Russia, which has made modifications in its laws in the field of privacy over the years, has put into effect The Law on Personal Data, which includes new directions, for instance, regarding the cross-boarding transfer of the data, starting in 2022 [28].

Turkiye: Turkiye has been using the Personal Data Protection Law (KVKK) since 2016. Before this regulation, a set of privacy laws based on the protection of personal data were not implemented [36]. KVKK was not constructed with GDPR as it was enacted earlier [35].

United Kingdom: The United Kingdom, which left the European Union in 2020, adopts and implements the UK General Data Protection Regulation (UK GDPR) as data protection regulations [32]. GDPR and UK GDPR contain parallel regulations [37].

United States: Privacy in the United States is not governed by a single overarching law or regulation. Instead, a collection of federal privacy laws covers different aspects of privacy. The most related to online consumers, California's Consumer Privacy Act (CCPA) includes the most comprehensive regulations regarding cookie control [38]. Similarly, the State of Delaware has protected the privacy of its citizens with the cookie laws it has legalized in the Personal Data Privacy Act (DPDPA) [39].

Overall each country mentioned above and subject to this study mandates the protection of individuals' information and their data and therefore legalizes consent implementations. They all emphasize transparent practices in personal information collected. While Brazil and Japan are not specific about the language clarity of cookie consent notices, other countries require that consent be created in a way that the user can understand. User consent and control are clauses in the data protection regulations of all these nine countries and give users the right to accept or reject. While Japan does not explicitly address cookies, it highlights user consent for personal data handling. In the US, states that implement cookie laws enforce user notification about cookie collection, yet not all states adopt legislation regarding cookies. We note that in our study, the US remote connection was only used for analyzing the websites of some of the countries as a third country to verify some of the results. So, the impact of the US privacy regulations was not a direct focus of this work.

3.2 Data Collection

We built a tool designed to extract cookie consent notices from the top 500 most visited websites located in Brazil, Bulgaria, Germany, Italy, Japan, Russia, Turkey, and the United Kingdom. We used the list provided by Tranco [33] to identify the most visited websites for each country stated and omitted standard domains such as .com, and .net to ensure that the target audience of the website and the country it is being evaluated for matches. The evaluation phase consisted of two levels, namely domestic and international. In the initial phase, we established connections within the target country and navigated to the respective websites to collect data. Subsequently, we behaved as an external user, simulated access from outside the country, and gathered further data. We provided all the connections we made with a consistent VPN. Through careful checks performed during the scanning process, we ensured our presence within the specified country. Each website was accessed through an incognito tab, allowing for a fresh user profile for every visit.

Due to the number of websites exceeding the possibility

for manual computation, we used Selenium for automated data collection, we preferred Firefox (Version 110.0) as the browser thanks to its solid stability with automated tools. We conducted the crawling between March and May in 2023.

We have conducted a crawling process that involved 10,000 visits (4,000 local, 4,000 remote from Turkiye, 2,000 remote from the US) for a total of 4,000 websites from 8 different countries including both local and remote connections. Among these crawls, 76.25%, 77.9%, and 68.95% of websites were loaded with local, remote from Turkiye, and remote from the US connections, respectively. Also, of the total dataset, 37% (1511) included a cookie consent notice as a banner as part of the website's privacy policy. And, the websites that were not loaded could not be accessed either due to being geographically blocked or having a temporary server problem.

In order to collect the details regarding the layout and content of the consent notices, we identified names used for a cookie banner as part of the technical design and created a pool of possible HTML element names. We ensured that the most popular third-party cookie policy banner providers and a variety of components were included in the pool. Later, we executed a second-level control, taking the text of the banner and searching for the existence of privacy policy-related words. We conducted this control by creating a pool of words and then pursued the identification of clickable texts and buttons in the banner, ensuring that it is related to obtaining the user's consent on privacy. We created three pools, one for accepting, one for rejecting, and one for viewing in-depth privacy settings offered by the website. For matching elements, we fetched the exact clickable text within the element for later evaluation. Moreover, if a clickable element related to rejecting the consent exists, we collected the number of cookies again after rejecting the policy to see whether a change was observed. The following subsections describe the attributes in detail. A high-level architectural view of the tool is provided in Figure 3 and the general flow of the process is given in Algorithm 1.

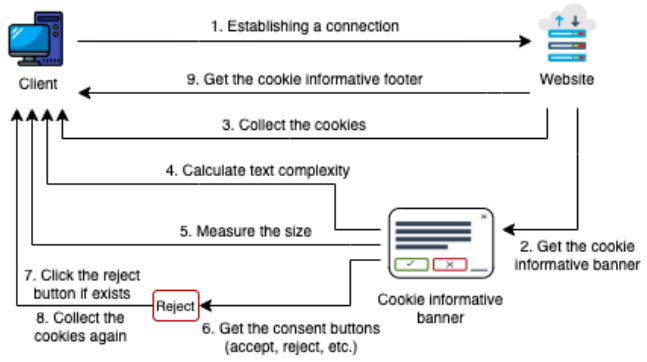


Figure 3: Flow of the automated tool.

Algorithm 1 Detection of Consent Notices

Step 1 and Step 2: Identify HTML Elements of Consent Notices and Privacy Policy-Related Words
Define a list of XPaths to search for banners
paths ← ["//*[contains(@role, 'dialog')]", "//*[contains(@role, 'alert')]", ...]
Create an empty list to store identified banner elements
banner_elements ← []
Create a pool of privacy policy-related words
privacy_related_words ← ["privacy", "consent", "policy", "cookies", ...]
for *path* **in** *paths* **do**
    banner ← *driver.find_elements*(*By.XPATH*, *path*)
    for *x* **in** *banner* **do**
        banner_text ← *x.text.lower*()
        translate_to_english(banner_text)
        for *word* **in** *privacy_related_words* **do**
            if *word* **in** *banner_text* **then**
                Append *x* to *banner_elements*
                This banner is related to privacy, process it further
                break
Step 3: Identify Clickable Text and Buttons in the Banner
Create word pools for accepting, rejecting, and viewing privacy settings
accept_words ← ["Accept", "Agree", "Allow", ...]
reject_words ← ["Reject", "Deny", "Decline", ...]
settings_words ← ["Settings", "Preferences", "Manage", ...]
for *banner_element* **in** *banner_elements* **do**
    clickable_texts ← *get_clickable_texts*(*banner_element*)
    for *text* **in** *clickable_texts* **do**
        if *text* **in** *accept_words* **then**
            Process accept button accordingly
        else if *text* **in** *reject_words* **then**
            Process reject button accordingly
        else if *text* **in** *settings_words* **then**
            Process settings button accordingly
Step 4: Check for Cookie Changes After Rejecting Consent
if "Reject" **in** *clickable_texts* **then**
    cookies_before_reject ← *get_cookies*()
    simulate_reject_click()
    cookies_after_reject ← *get_cookies*()
    if *cookies_before_reject* ≠ *cookies_after_reject* **then**
        Change in cookies observed after consent is denied

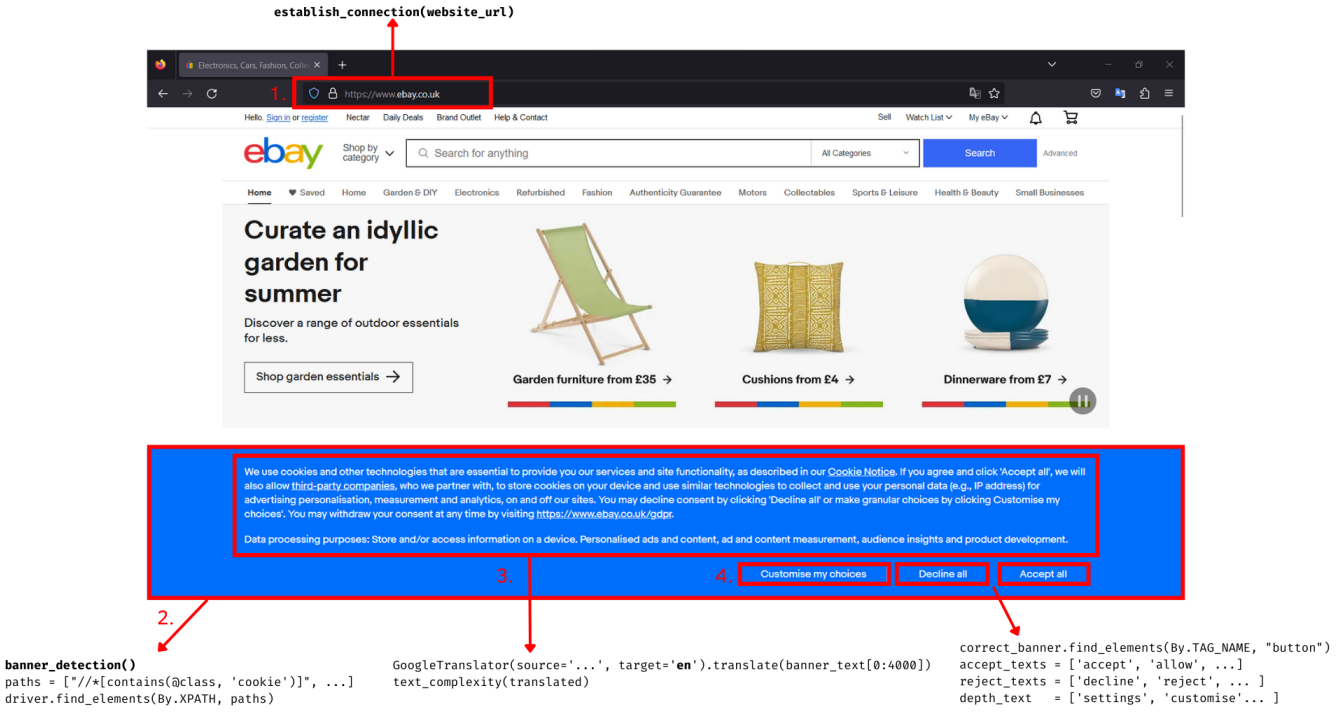


Figure 4: Overview of the detection of privacy notices and elements; Steps 1 and 2 correspond to privacy banner identification, and Steps 3 and 4 correspond to privacy policy identification.

3.3 Inspection and Verification

We conducted the manual inspection process following data collection, ensuring that the scan-derived data was thoroughly prepared for analysis. We formed control groups for each country to be checked manually and also included edge cases as a part of this group. These control groups were formed according to data being false positive (where we found cookie informative banners while there are none) and/or negative (and vice versa). For manual checks, the same procedure described above is computed. First, the accessibility of the website and the existence of a privacy-related banner is evaluated. Following, text analysis is computed, using the component of the code we developed manually, providing the text as an input and getting statistics as an output. Options provided to the user as a part of the banner and layout details are also collected manually using the inspection tool of the browser. Lastly, further privacy notices are checked to see if any additional notice is provided as a footer.

Utilizing a feature in our code, we captured screenshots of web pages in instances where no consent notice was encountered during the scanning. Thereafter, we reviewed these screenshots, using them to fix any inaccuracies. Overall, automated and manual checks not only complied with each other but also supported the validity of the data collected and thus, the work conducted.

3.4 Measurement Metrics

3.4.1 Content of the Data

We established a three-stage investigation mechanism on the user-centric privacy policies of websites, which is also visualized in Figure 4. The content of the three-stage procedure can be briefly described as follows:

1. Privacy Banner Identification: Checking if the website is accessible and if loaded successfully, whether a privacy-related banner is shown to the user (corresponding to 1 in Figure 4).

2. Privacy Policy Identification: Investigation of the comprehensibility and clearness of the text shown to the user if a banner stating the policy followed by the website exists. Along with the text, the options displayed, such as accepting or rejecting to give consent or viewing additional information. Moreover, information on the layout of the banner (corresponding to 2, 3, and 4 in Figure 4).

3. Further Privacy Notice Identification: Existence of further privacy policy-related notices on the website.

Regarding the number of cookies integrated into the stages described above, we also focused on quantitative data regarding the cookies taken, before and after rejecting the consent

notices. Nevertheless, we were able to measure the number of cookies after rejection only if the website provided a rejection option to the user.

3.4.2 Depth of Rejection

Another new metric named *depth* is computed based on the existing data on the options provided to the user as a part of the cookie consent notices. Depth is important to give insights into how easy it is for the users to reject the privacy policy offered by the websites. This metric classifies the depth into three categories; namely *no reject option*, *a reject button exists*, and *further reject options* (e.g., Settings). No reject option category is used for cases where there is no cookie banner or option offered to the user as a part of a privacy notice. On the other hand, a reject button exists means that users can reject the cookies with a single click, and consequently further reject options indicate the user cannot reject with a single click but have further options offered, which may result in the rejection of the consent with two or more clicks. Figure 5 presents the use of depth metrics within the research.

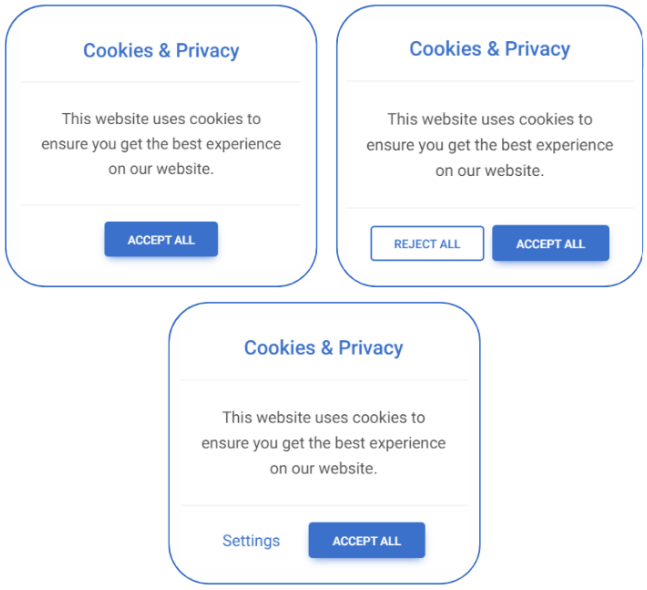
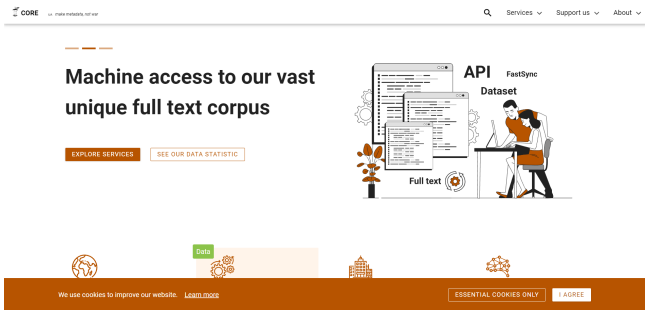


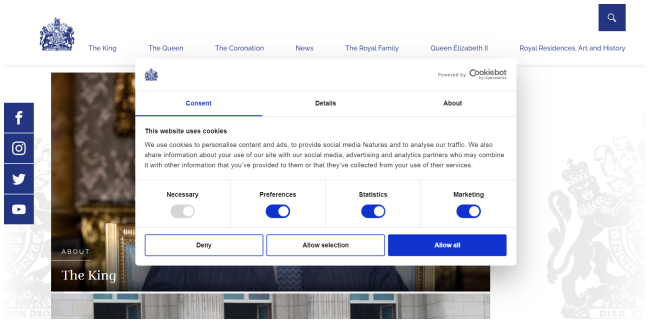
Figure 5: Visual representation of different depth levels observed in privacy notices.

3.4.3 Layout of the Banner

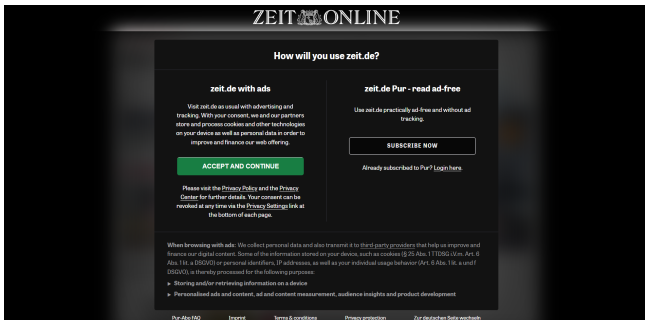
We have also developed a novel metric to evaluate the layout of the banner. This new metric named banner classification is determined from the data collected on the layout of the banner. Specifically, the size information of the banner is utilized to take the ratio of the banner to the browser. As also shown in Figure 6, banners that are smaller than a quarter of the view are classified as *small* (Figure 6a), while banners between quarter and half of the view are classified as *medium* (Figure 6b), and banners larger than half of the view are classified as *large* (Figure 6c). The size information indicates the level of transparency on the website regarding the collection of cookies and the effectiveness of the notice provided, which directly impacts the user experience.



(a) Small



(b) Medium



(c) Large

Figure 6: Examples for classification conducted regarding the layout.

3.4.4 Banner Text Analysis

Another crucial part of the data collection that needs to be further discussed is the identification of the level of complexity, which plays a key role in the easiness of understanding the banner text. The reason we analyzed only the cookie banners is that they are constructing the main behavior of the users. They are the first thing that would catch one's eyes and shape the users' demeanor.

One of the ways to determine the complexity of text is to calculate its vocabulary richness. However, this method forces us to assume there must be a correlation between the complex words and the difficulty of understanding a text.

In contrast to the assumption above, Yasseri et al. [43] argue that Dickens' books have more specific and complex words but are easier to understand in comparison to simple Wikipedia articles online. In fact, they conclude that vocabulary richness indices are not enough to determine whether a text is hard to comprehend, one must look for other aspects such as the complexity indices that include sentences as well.

Hence, we decided to utilize a more detailed metric called Gunning Fog Index [15] to measure the complexity of texts by including the fundamentals of a paragraph: its sentences, and the complex words inside, which is formulated as:

$$F = 0.4(W/S + (100 * CW/W)), \quad (1)$$

where W, CW, S are the total number of words, complex words, and sentences, respectively [1].

We fetched the texts directly from the detected cookie banners, and calculated their complexities at the same time by tokenizing sentences and hyphenating words.

The text complexity of banners for different languages was analyzed through the main language, English. Other languages were translated by ensuring and conserving their true meanings so that there is no loss of meaning in all manners. We decided to conduct this analysis with a single language (i.e., English) to obtain objective results. For instance, Japanese and Turkish are agglutinative languages, while German and English are Indo-European. Therefore, with English, we provided a universal outcome for all to make it fairer to analyze and compare with each other.

According to the index, complex words are the ones that have at least three syllables. The result shows the target audience of the corresponding text, where the fog index being 9-12 means that the text is for high school students, 13-16 for university students, and above for graduate level students [11]. Any fog index result above 13 is thus accepted to be difficult to understand at first reading.

3.5 Ethical Considerations

All data collected in this study are publicly visible elements of websites. Neither any private data of any person or institution was used nor shared. Therefore, our work does not lead to any ethical violations or concerns.

4 Data Analysis and Results

This study sought to understand whether privacy notices and the options they contain differ in various countries across the world. It also checks for any privacy-related links in the footers of websites. The scans were completed both from the country where the domain belongs to the website and from abroad, and the results can be seen in Table 1. It is beneficial to clarify the statistics for the false negatives and false positives that our tool has made a successful crawling by producing 2.1% and 2.4%, respectively, which provides us a small but nice-to-have space to dig deeper for manual inspection and verification.

4.1 RQ1: Privacy Consents of Websites in Various Countries

Table 1 shows that in terms of the existence of cookie informative banners: the UK has a certain lead in both local and remote connections. 70.64% of the remote and 86.66% of the locally connected websites contain a cookie banner to inform users and ask for their consent. Following the UK, Germany and Italy have good grades in terms of notifying users when entering their websites. They both have at least a 60 percent rate to contain a cookie banner and banner sizes are not like other countries' banner implementations where relatively small sizes predominate. Regarding this trio, Germany shows its difference in the rate of accepting buttons. Almost all of the German cookie banners include an accept button for users to proceed to the website. In addition, Germany also has the most amount of cookie-informative footers. It can be said that Italy and the United Kingdom, especially the 14% of the remotely linked UK websites, do not pay much attention to the footers as they include a non-negligible amount of banners.

On the other hand, Japan holds its position at the bottom by having the poorest banner and footer rates of 8.04% local & 9.31% remote, and 17.59% local & 22.8% remote connections, respectively. Russia could take place just above Japan because Russian websites are also not privacy-consent-mannered but have a few websites where users can reject the cookies. Looking at Russia and Japan, which were chosen as two of the intriguing G20 countries, it can be seen that both countries do not demonstrate effective obligations towards online privacy.

The other three countries, Brazil, Bulgaria, and Turkiye, share the middle part where they all have close banner and footer existence rates (except remotely connected .br websites with 51.18%).

In addition to the results of each country, connections from different locations do not have a solid pattern. For instance, except for text complexity and reject buttons ratio, locally connected UK websites have better results than remotely connected ones. German websites that are locally connected tend to provide more favorable outcomes compared to those that are remotely connected, except for accept buttons and depth of rejection (i.e., further consent options). On the other hand, Brazilian and Bulgarian websites have slightly better results when they are locally connected. Additionally, if we take into account the exact locations of these connections, there

Table 1: Results on how well websites inform their users about cookies.

Countries	Cookie Informative Banners (%)[1]	Accept Buttons (%)[2]	Reject Buttons (%)[2]	Further Consent Options (%)[2 5]	Average Text Complexity	Dominant Banner Size[3]	Cookie Informative Footers (%)[1 6]
Brazil	42.89	62.16	8.98	12.16	11.95	Small (93%)	29.4
Brazil (rc[4])	52.49	79	18	8.5	12.59	Small (94%)	51.18
Bulgaria	44.31	63.59	6.15	17.43	11.53	Small (86%)	36.6
Bulgaria (rc[4])	46.54	68.31	5.94	19.8	12.05	Small (75%)	32.2
Germany	67.07	98.9	34.55	21.81	12.8	Medium (40%)	83.33
Germany (rc[4])	63.09	99.09	31.13	25.47	13.13	Medium (46%)	79.5
Italy	60.05	80.87	27.83	41.73	14.49	Small (50%)	42.6
Italy (rc[4])	65.9	89.96	32.49	40.92	15.29	Small (39%)	42.4
Japan	8.04	68.75	6.25	37.5	11.29	Small (87%)	17.59
Japan (rc[4])	9.31	52.17	8.63	21.73	12.92	Small (82%)	22.8
Russia	28.78	43.1	0.86	4.31	11.20	Small (92%)	30.59
Russia (rc[4])	27.2	49.01	1.96	5.88	10.99	Small (95%)	29.2
Turkiye	36.44	57.92	12.19	12.19	11.22	Small (92%)	37.8
Turkiye (rc[4])	42.15	48.88	5	28.88	12.95	Small (77%)	38.47
UK	86.66	82.69	16.21	41.48	11.36	Small (61%)	54.6
UK (rc[4])	70.64	79.72	16.55	40.87	10.64	Small (67%)	14.35

[1] The ratio of the corresponding component to all successfully loaded websites.
[2] The ratio of the corresponding component to number of banners.
[3] Small: Covering at most the quarter of the screen. Medium: Covering more than a quarter but less than half of the screen. Large: Covering more than half of the screen
[4] rc: Represents "Remote connection". Remote connection to .tr websites is from London, UK. All other TLDs' remote connections are from another location (e.g., Turkiye).
[5] Depth of rejection.
[6] Cookie and privacy policy links located in the footers of websites.

is no clear-cut differentiation. Bulgaria, Germany, Italy, and the UK, which mainly adopt GDPR, have different results in different locations in terms of being more privacy-mannered. Bulgarian and Italian websites show more consent notices when connected remotely from a non-EU location (Istanbul, Turkey), while in Germany and the UK, more cookie banners are shown on local connections.

Effect of Country Selection for Remote Crawls: In order to enrich the scope of the work conducted, we investigated the effect of the selected country used for remote crawls. We selected the United States as a consistent third country for remote crawls and repeated the crawls for Japan, Russia, Turkiye, and the United Kingdom. When we collectively investigated the results, which are represented in Table 2, we identified worse ratios for presenting a cookie banner along with accept and reject buttons for Japan, Turkiye, and the United Kingdom. On the other hand, we did not observe a

Table 2: Statistics for the remote crawls done from the US.

Countries	Cookie Banner Existence (%)	Accept Button Rate (%)	Reject Button Rate (%)	Average Text Complexity (%)
Japan	9.05	38.10	4.76	12.91
Russia	29.71	51.49	1.98	11.04
Turkiye	31.2	41.66	6.41	12.35
United Kingdom	48.10	70.30	22.77	11.16

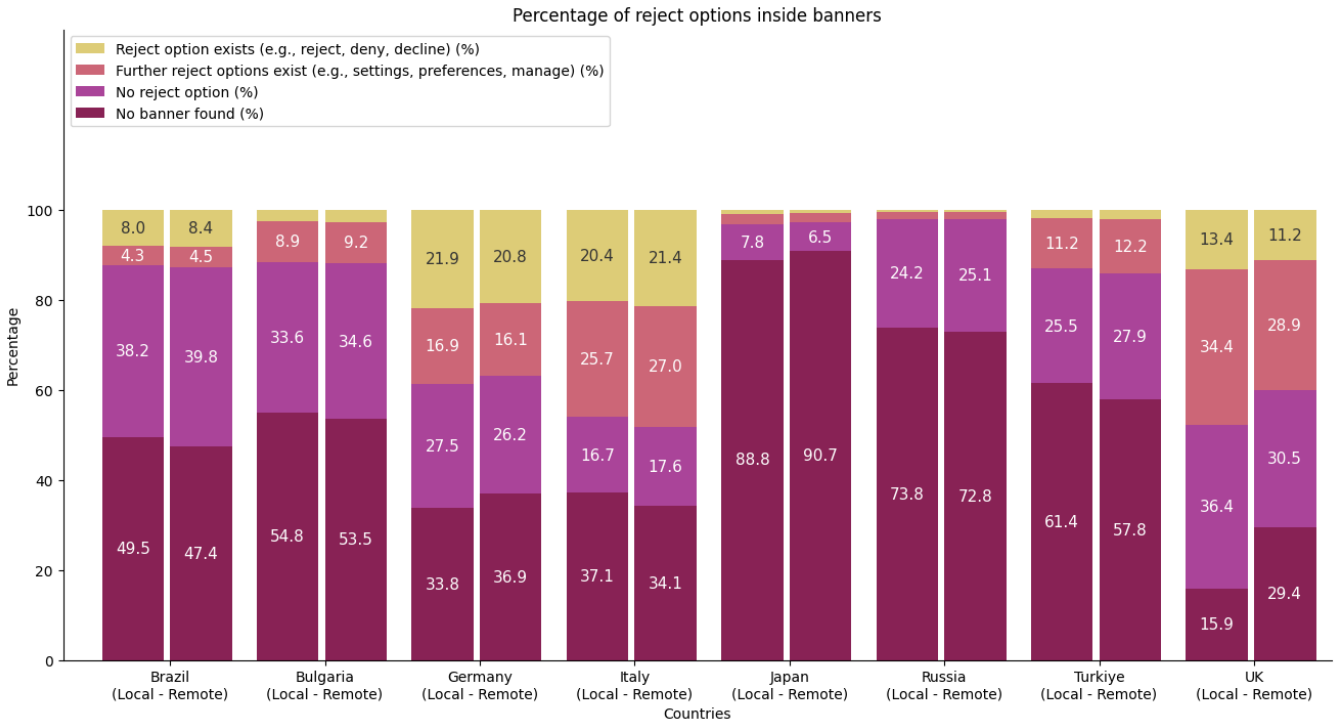


Figure 7: Reject options inside the cookie informative banners: Bars are grouped according to the countries that the websites belong to. Each country's left bar represents the results coming from local connections, and the right bar represents the results coming from remote connections.

significant difference for Russia.

The most striking statistics we observed were for the banner presence rates of the United Kingdom, showing up to be 48.10% when the connection is made from the US and 70.64% when from Turkiye. Additionally, the accept button rates for the privacy banners found in Japan were 52.17% and 37.10% for connections made from the US and Turkiye, respectively. On the other hand, we identified that Russia is demonstrating stable behavior in privacy for traffic coming from varying countries. These results can be interpreted from the perspective of the privacy legislation in Turkiye being similar to GDPR as they have historical ties to the EU. This might suggest an evaluation of Turkiye and the EU in the same group, thus obtaining better statistics when connections are done from Turkiye. Such evaluation also implies that European websites are more careful in privacy for traffic coming from other European countries because of the recent regulations. Another conclusion that can be inferred is that the difference we observed between connections from the US and Turkiye may be an outcome of not having a consensus like the EU's GDPR in the US. Using the US connection allowed us to verify that websites change behavior by country.

Language Settings of the Browser: Another point of investigation we made was the impact of the language settings of the browser. For this purpose, we examined the countries within the scope of this research having languages with different alphabets, namely Japan and Russia, making connections using VPN. The findings we obtained from this study did not show any significant difference; hence we concluded that the language settings of the browser are not dependent on the presentation of the privacy policy.

4.1.1 Reject options

Apart from the results in Table 1, Figure 7 shows the three different cookie rejection options. Further, reject options can be explained as having special *settings* buttons where the cookie acceptance options can be customized.

United Kingdom websites are on top by having the most amount of reject buttons with the second highest further options ratio. Both UK local and remote connections share these results. Germany and Italy are the followers by having reject options for more than half of their banners in a more evenly distributed way than other countries. They are followed by Bulgaria, Brazil, and Turkiye. Bulgarian websites are almost identical with both connections by having a close amount of reject buttons and further options. Turkish websites are similar to Bulgarian ones in terms of having more further options than just reject buttons. Brazilian websites have more reject buttons with no further depth contrary to the previous two. Finally, Japan and Russia take the last two places. Almost

70% Japanese and more than 92% of Russian websites lack reject options to provide users with a secure and reliable environment. In addition, the results of the crawling from the US connection were similar compared to the aforementioned results, except the UK websites. Higher reject button rates observed in the UK, despite the lower banner rates, show that websites that do not provide a reject option when connected from the UK are not providing a banner at all when connected from the US.

Table 3: Number of websites that are collecting cookies before and after clicking the reject button to observe if users *actually* reject them all or not. BC: Before clicking the reject button, AC: After clicking the reject button.

Countries	BC	AC	Countries	BC	AC
Brazil	32	1	Brazil (rc[1])	36	0
Bulgaria	12	1	Bulgaria (rc[1])	12	0
Germany	95	1	Germany (rc[1])	82	1
Italy	70	0	Italy (rc[1])	84	0
Japan	1	0	Japan (rc[1])	2	0
Russia	1	0	Russia (rc[1])	2	0
Turkiye	20	2	Turkiye (rc[1])	9	0
UK	47	3	UK (rc[1])	49	2

[1] rc: Represents "Remote connection". Remote connection to .tr websites is from London, UK. All other TLDs' remote connections are from Istanbul, TR.

Figure 7 shows us that for six countries, reject options' variety and amount increases when they are connected from another location (e.g., Turkiye) in comparison to their hometown. Germany has the same amount of reject options for both connections. UK websites are the only ones that resulted better with the local connection. Although this might be understandable for Brazil, Russia, or Japan which are not adopting GDPR for their data privacy regulations, it is also a surprise for countries such as Bulgaria, Italy, or Germany where people usually do not expect to see many consent options when they are connected outside the EU.

Table 3 demonstrates the before and after the state of clicking reject buttons of those which include. The presence of reject buttons within cookie banners allows users to *decline* the use of cookies with their free will. According to this information, all results are low. While expecting to see that all reject buttons are fully functional and do the desired outcome as refusing all cookies, only 7 of them worked on all websites for local connections, and 2 for remote connections, which is also undesirable to see. In fact, the number of cookies on most of the websites increased after clicking the reject buttons. One possibility is that they use them to keep track of whether users have closed the informative banner and thus ensure that it does not appear again.

4.1.2 Text Complexity of Banners

Text complexities of cookie informative banners were calculated with the Gunning Fog Index (see Figure 8). They were calculated by gathering from cookie informative banners and translated into English.

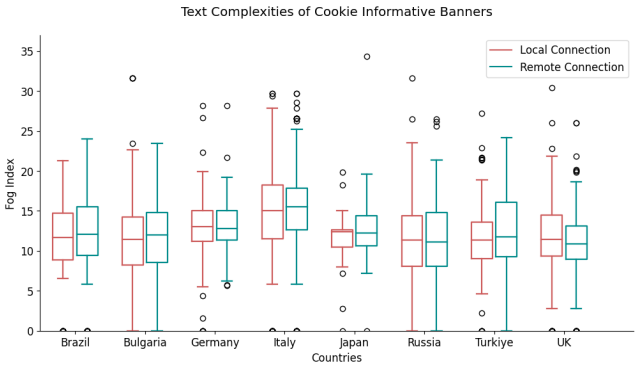


Figure 8: Boxplot for text complexities of cookie informative banners: Results are measured with Gunning Fog Index. The bottom and top quartiles are 25^{th} and 75^{th} percentiles, while the median is in between. Whiskers below and above show the minimum and maximum values except the outliers.

On average, Italian websites have the most complex texts inside their banners. Germany comes second but not having as much variety as Italy does. The UK, on the contrary, has the least complex texts, especially for local connections. Despite having the most amount of banners and variety in reject options (see Table 1), we can say that their banners' purpose is to deliver the information as simply as possible. Because, the 10.64 complexity rate is relatively easy, while others' complexities go from medium to difficult levels [11].

Regarding the difference between local and remote connections, Turkiye has fluctuated results for remote connection, starting from 0 to approx. 25. It seems that Japan has also a significant difference between the two connection types. However, it has so less banners on both sides to consider, thus, it is hard to comment on them. Other countries' websites are close to each other and there is no pattern for different connections.

There is not much of a difference in average values between the two connection types when we examine them pairwise. Also, we observed that there was no significant change in the text complexity of the text in cookie banners when connecting remotely from the US to other countries.

In conclusion for the first research question, user-centered privacy is mostly appreciated by developed European countries, such as Germany, Italy, and the United Kingdom. These three countries lead the results in terms of having the most amount of cookie informative banners and providing consent to users to accept or reject their cookies. Brazil, Bulgaria, and Turkiye come after the first trio. While nearly half of Brazilian, and more than half of Turkish and Bulgarian websites

lack banners, those banners are predominantly small and lack reject buttons as well. Lastly, Russian and Japanese websites do not represent any term of privacy awareness for the users.

4.2 RQ2: Geographical Impact

Regarding our second research question, we selected suitable G20 countries from the American, Asian, and European continents, which could yield interesting results when compared. The results indicate that Japan provides considerably less information about the cookie collection process than other countries. Following that, cookie banners were found on only 28% of the Russian websites scanned. On the European side, an increase in these informative banners is marked. However, the results acquired from European countries indicate that there are almost 10-20% variation intervals and they all contain privacy-related links at different rates.

For example, although Brazil and Bulgaria are in different regions and subject to different laws, the user notification rates are nearly the same. Therefore, it is not appropriate to establish a direct correlation. Although it is believed that neighboring countries interact with each other through both immigration [12] and trade [31], so they may share similar characteristics and cultures, it is not necessarily the case when it comes to privacy.

4.3 RQ3: Countries Adhering to Same Regulations

We collected data from the 500 most visited websites in eight countries throughout our research on user-centric privacy practices. This data is also beneficial for the evaluation of countries following the same data protection regulations and giving an answer to one of our research questions. Three of the countries investigated during the research are part of the European Union; namely Bulgaria, Germany, and Italy. Moreover, despite the United Kingdom having left the union, the country still adheres to the General Data Protection Regulation (GDPR) of the EU, UK GDPR being in effect. Therefore, the results obtained from these four countries imply inferences on whether differences exist across the countries adhering to the same data protection regulation. Figure 9 filters the results acquired for these four countries on the existence of accept and reject buttons and displays these results as a graph for better visual interpretation.

As displayed in Figure 9, significant differences exist in the characteristics of the privacy consent notices provided to users in these countries. When supported by the results stated in Table 1, Germany takes the lead on the accept button provision rate, being 99.09%. Italy and the UK follow Germany with slightly lower rates, respectively 80.87% and 82.69%. Nevertheless, Bulgaria demonstrates an unlike characteristic with 63.59%. Even the difference obtained for the existence of accept buttons indicates that there might be differences in

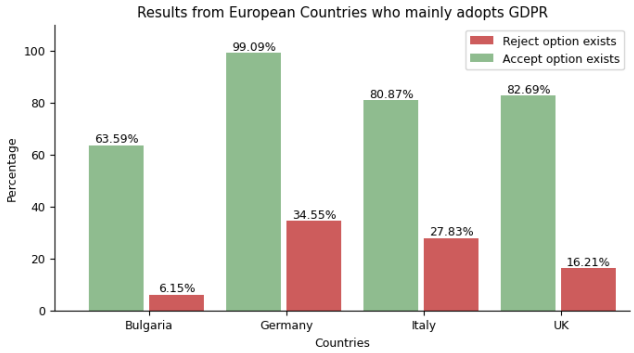


Figure 9: Results on accept and reject button filtered for the countries adhered to GDPR.

practice even though the regulations are the same. Moreover, the significant differences across Bulgaria and Germany on the existence of a reject button, being 6.15% versus 34.55% together with Italy and Germany on further consent options, being 41.73% versus 21.81% advocates the statement that practices do show differences in countries following the same protection regulations.

Therefore, the question on the similarity of cookie consent notices can clearly be answered as even though the countries adhere to the same regulations, the application of these regulations does demonstrate clear variance. Furthermore, this variance extends up to more than 25% differences for the countries considered for this research.

5 Discussion

The results obtained from collected data suggest that user-centered privacy perspectives across countries do differ mostly on the aspect of the options they are providing to the users themselves. These options can be briefly identified as accepting the policy of the website, rejecting the policy, and viewing further options on the coverage and details of the applied policy. The analysis for which the statistics are discussed below is conducted among 77.97% of the websites that are loaded successfully and 44.84% of the loaded websites that have a privacy-related banner.

As the findings of our extensive analysis state, the difference in the rate of acceptance option provided shows a variance of 55.95% in the countries examined, with Germany taking the lead with 99.09% and Russia being the worst country with 43.1%. When it comes to the rate of rejection, on the other hand, the variance observed decreases to 34.59%; again the leading country is Germany with 34.55% and the worst country is Russia with only 0.86%. These outcomes also indicate that users are mostly unable to directly reject the privacy policy of the website; even in the leading country Germany. As a last point of determination, viewing further options also shows a variance of 37.42% across the countries

examined. The lead country changes as Italy with 41.73% for this aspect while the worst country stood steady being Russia with 4.31%. From the results stated above, it can be concluded that either the data protection law enforced in Russia is not satisfactory or it has no effect when it comes to implementation. Furthermore, it can be stated that European countries have better results, indicating that GDPR is relatively successfully implemented.

On the other hand, the investigation computed on the geographical influence on privacy-related practices resulted in significant differences between cultural zones. Russia and Japan, representing the eastern cultural zone, had the lowest results on the statement of the privacy notices and providing options on the notice to the users, whereas Europe had the highest results. The Middle East and South America showed similar characteristics, finding a place in between the highest and lowest results. Nevertheless, these cultural zones have no strict borders between countries. For instance, Bulgaria and Turkiye's results are similar to each other. Therefore, it can be stated that although some inferences can be made regarding different geographical locations, it is not appropriate to categorize countries in line with either zones or borders they belong to or share.

Furthermore, it is clearly visible in the outcomes that a significant amount of websites do not offer an option to the users to reject the privacy policy they are presenting. However, Western Europe still differentiates from the rest of the world in the options provided to the users. Evaluating the percentage of direct rejection, Germany and Italy take the lead with 34.5% and 27.8% respectively. In addition, Italy and the UK take the lead in providing further reject options such as viewing the settings or changing preferences with 41.7% and 41.5%. Although European websites seem to offer more options on the privacy policies they offer, the outcomes suggest that there is still a need for improvement.

The work conducted on the similarities in countries adhering to the same data protection regulations resulted in a specialized comparison across the EU with an addition of the UK due to their common grounds on the regulations. The results obtained show an existence of variance in the banner layouts and the options provided being part of the banner. Therefore, it can be inferred that although the regulations have common grounds, applications may show differences across countries. The fact that Bulgaria and Turkiye have similar results, stated as an answer to geographical influence is also supportive of this aspect of the research. Instead of sharing similar results with other European countries that enforce GDPR, Bulgaria shares a similar result with its neighboring country Turkiye.

As a last point of discussion, when we remotely connected to countries and used the US as our constant reference point, we noticed an interesting trend. Specifically, we found that when a user connected from the US, the possibility of encountering cookie banners on European websites was lower compared to connecting from countries in Europe. In contrast, the situation remained relatively consistent when connecting from the US to websites located in other parts of the world. The fact that this difference is seen between the US, which does not have a general cookie law, and the European Union, which has adopted GDPR, which has strict cookie rules, shows how important it is for citizens that authorities take precautions since it changes and impact attitudes worldwide over cookie privacy consent notices.

5.1 Limitations

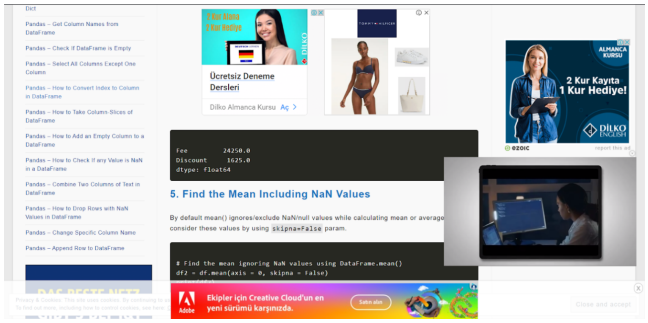
Due to the extent of the research conducted, some edge cases had to be checked manually. These edge cases can be briefly stated where irrelevant clickable text is identified as accept and reject button texts. Despite a large pool of components and words has been created for the automatic data collection phase, such situations have been encountered due to the diversity in cookie consent banners and the options offered as a part of them. Moreover, diversity in the component names used for cookie consent banners increased the amount of preliminary research that has to be conducted to catch all types of banners. Due to the distinctive implementation of the cookie banners on the websites, some cases still existed where Selenium had difficulty accessing the banner, text, or options. Examples for such cases are shown in Figure 10a, 10b, and 10c . On the other hand, the instability of VPN connections caused delays and repetitions in the data collection phase.

6 Conclusion

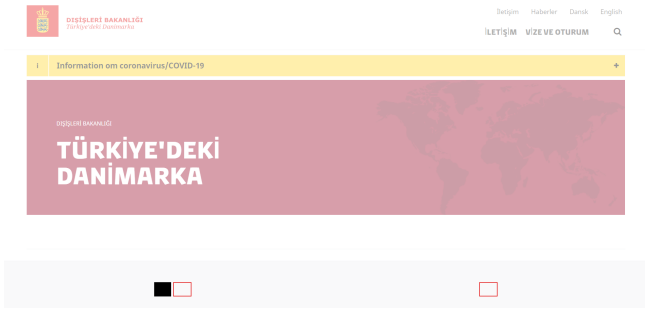
As the concern regarding privacy is increasingly central to one's data protection in online settings, it is essential to comprehend how different countries around the world inform their users about this subject and acquire their consent for web browsing. This study indicated the applications of privacy notices by analyzing the 500 most popular websites of 8 different countries and discussed the variances across these countries. For this purpose, an automated tool for large-scale data collection is implemented, covering banner layout, privacy notice text, and the options provided to the user such as accepting, rejecting, or viewing details of the privacy policy.

We discovered that many countries were insufficient to display effective privacy notices with their cookie consents, regardless of the privacy protection laws they were based on and their locations. While there was no increase in cookie consent notice existence when remote connections from different perspectives (i.e., Turkiye and the US) were established, we even observed that cookie banner existence decreased when accessing European websites from the US. In countries other than Bulgaria, Germany, and the UK, the rate of presenting a banner to the user that cookies will be collected is below 50%. In addition, the maximum rate of giving the user the right to

(a) Cookie banner implementation with no information.



(b) Cookie banner implementation behind advertisements.



(c) Cookie banner implementation without text and options.

Figure 10: Examples of confusing cookie banner implementation.

reject across the investigated countries is 35% and this is provided by Germany. In the remaining banners, either the user is given the option to accept only, or the cookies are collected without consent and giving any option. The average rate of those who do not put their privacy policy in the footer of their website is 60%. These findings indicate that user privacy is not respected by a majority of websites, putting user data at risk of being exposed.

Users are generally not limited to navigating websites only available in their home country, they can access websites from all over the world. The significance of this study is to demonstrate to users how their data is approached while browsing online platforms from different countries. It is envisaged that the reader will dissect the issue of failure to provide the information and rights regarding cookie collection from a wider perspective with a worldwide study.

Future research in privacy notices around the world can attempt to link with the privacy cultures of the regions by scanning more countries. A more comprehensive study from a sociological point of view can also provide privacy and different connections. We have to *accept all* that data sharing is growing and we should raise awareness about this matter.

Acknowledgements

We thank the anonymous reviewers and our shepherd for their helpful feedback and time. This work was partially supported by the US National Science Foundation (Awards: 2039606, 2219920), Cyber Florida, and Microsoft. The views expressed are those of the authors only, not of the funding agencies.

References

[1] Assessing the Level of Your Language - The Fog Index. https://www.courts.ca.gov/partners/documents/Assessing.pdf.

[2] AKSU, H., BABUN, L., CONTI, M., TOLOMEI, G., AND ULUAGAC, S. Advertising in the iot era: Vision and challenges. *IEEE Communications Magazine* (April 2018), 1–7.

[3] BIANCO, G. *An empirical analysis of consumer response to Google's decision of phasing out third party cookies*. PhD thesis, 2020.

[4] BOLDYREVA, E. Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. pp. 91–102.

[5] A Practical Guide to Data Privacy Laws by Country - Brazil. https://www.caseiq.com/resources/a-practical-guide-to-data-privacy-laws-by-country/#Brazil.

[6] Bulgaria - Data Protection Overview. https://www.dataguidance.com/notes/bulgaria-data-protection-overview.

[7] CARPINETO C., L. R. D., AND ROMANO, G. Automatic Assessment of Website Compliance to the European Cookie Law with CooLCheck. In *In Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society* (2016), ACM.

[8] CHEN, G., COX, J. H., ULUAGAC, S., AND COPELAND, J. A. In-depth survey of digital advertising technologies. *IEEE Communications Surveys Tutorials 18*, 3 (3rd quarter 2016), 2124–2148.

[9] CHEN, G., COX, J. H., ULUAGAC, S., AND COPELAND, J. A. In-depth survey of digital advertising technologies. *IEEE Communications Surveys & Tutorials 18*, 3 (2016), 2124–2148.

[10] DEGELING, M., UTZ, C., LENTZSCH, C., HOSSEINI, H., SCHAUB, F., AND HOLZ, T. We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy.

[11] ELEYAN, D., OTHMAN, A., AND ELEYAN, A. Enhancing Software Comments Readability Using Flesch Reading Ease Score. *Information 11* (2020), 6–7.

[12] EPSTEIN, G., AND GANG, I. Chapter 1 Migration and Culture. *Frontiers of Economics and Globalization 8* (2010), 1–21.

[13] A Practical Guide to Data Privacy Laws by Country - Germany. https://www.caseiq.com/resources/a-practical-guide-to-data-privacy-laws-by-country/#Germany.

[14] GRIGGIO, C., NOUWENS, M., AND KLOKMOSE, C. Caught in the Network: The Impact of WhatsApp's 2021 Privacy Policy Update on Users' Messaging App Ecosystems.

[15] GUNNING, R. *The Technique of Clear Writing*. New York: McGraw-Hill International Book Co., 1952.

[16] HORMOZI, A. M. Cookies and Privacy. *Information Systems Security 13* (2005), 51–59.

[17] Information to be provided where personal data are collected from the data subject. https://gdpr-info.eu/art-13-gdpr/.

[18] Italy - Data Protection Overview. https://www.dataguidance.com/notes/italy-data-protection-overview.

[19] Italy General Data Protection Regulation Overview. https://securiti.ai/italy-data-protection/.

[20] Japan - Data Protection Overview. https://www.dataguidance.com/notes/japan-data-protection-overview.

[21] KÖKCIYAN N., Y. P. PriGuardTool: A web-based tool to detect privacy violations semantically. In *Engineering Multi-Agent Systems* (2016).

[22] MARTINO TREVISAN, STEFANO TRAVERSO, E. B., AND MELLIA, M. 4 Years of EU Cookie Law: Results and Lessons Learned. In *Proceedings on Privacy Enhancing Technologies* (2019).

[23] MERITXELL BASART DOTRAS, P. B. R. Online privacy: Analyzing the use of cookies in web pages.

[24] MICHAEL KRETSCHMER, J. P., AND WEHRLE, K. Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. In *ACM Transactions on the Web* (2021), ACM.

[25] NOUWENS, M., LICCARDI, I., VEALE, M., KARGER, D. R., AND KAGAL, L. Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. *CoRR abs/2001.02479* (2020).

[26] PIERSON, J., AND HEYMAN, R. Social media and cookies: Challenges for online privacy. *info 13* (2011), 30–42.

[27] REHMAN, I. Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice* (2019).

[28] Russia - Data Protection Overview. https://www.dataguidance.com/notes/russia-data-protection-overview-0.

[29] SANCHEZ-ROLA, I., DELL'AMICO, M., KOTZIAS, P., BALZAROTTI, D., BILGE, L., VERVIER, P.-A., AND SANTOS, I. Can i opt out yet? gdpr and the global illusion of cookie control. Asia CCS '19, Association for Computing Machinery, p. 340–351.

[30] SANTOS, C., ROSSI, A., CHAMORRO, L. S., BONGARD-BLANCHY, K., AND ABU-SALMA, R. Cookie Banners, What's the Purpose?: Analyzing Cookie Banner Text Through a Legal Lens. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society* (2021), ACM.

[31] SOTSHANGANE, N. What Impact Globalization has on Cultural Diversity?

[32] The Data Protection Act. https://www.gov.uk/data-protection.

[33] Tranco. https://tranco-list.eu/.

[34] TREVISAN, M., TRAVERSO, S., BASSI, E., AND MELLIA, M. 4 Years of EU Cookie Law: Results and Lessons Learned. *Proceedings on Privacy Enhancing Technologies 2019* (2019), 126–145.

[35] Turkish Personal Data Protection Law No. 6698 and European General Data Protection Regulation. https://www.erdem-erdem.av.tr/en/insights/turkish-personal-data-protection-law-no.-6698-and-european-general-data-protection-regulation.

[36] Turkiye - Data Protection Overview. https://www.dataguidance.com/notes/turkey-data-protection-overview.

[37] UK - Data Protection Overview. https://www.dataguidance.com/notes/uk-data-protection-overview.

[38] Cookie control in the US. https://www.cookiebot.com/en/cookie-control/.

[39] Delaware Personal Data Privacy Act Compliance Guide. https://termageddon.com/delaware-personal-data-privacy-act-compliance-guide/.

[40] UTZ, C., DEGELING, M., FAHL, S., SCHAUB, F., AND HOLZ, T. (Un)informed Consent. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (2019), ACM.

[41] VARDARLIER, P., AND ZAFER, C. Social Media and Crisis Management: The Case Study of Cambridge Analytica. *Celal Bayar University Journal of Social Sciences* (2020), 31–44.

[42] WhatsApp Privacy Policy. https://www.whatsapp.com/legal/privacy-policy/.

[43] YASSERI, T., KORNAI, A., AND KERTÉSZ, J. A practical approach to language complexity: A wikipedia case study. *PloS one 7* (11 2012), e48386.