Analyzing Browser-Specific Cookie Functionalities and GDPR Compliance in Irish Websites

Ridhima Chhabra
School of Computing
Dublin City University
Dublin, Ireland
ridhima.chhabra2@mail.dcu.ie

Nikhil Kumar
School of Computing
Dublin City University
Dublin, Ireland
nikhil.kumar3@mail.dcu.ie

Dr Harshvardhan Pandit
School of Computing
Dublin City University
Dublin, Ireland
harshvardhan.pandit@dcu.ie

***Abstract*—Cookies are essential to internet browsing as they improve user experience, website functionality, and display of relevant ads. However, they also pose privacy risks, especially under strict legal frameworks like the ePrivacy Directive and the General Data Protection Regulation (GDPR). This research examines the types and purposes of cookies used by Irish websites, focusing on GDPR compliance and privacy implications. By comparing data from Irish websites with the Open Cookie Database, we provide a comprehensive analysis of cookie practices. We also propose recommendations to enhance user understanding and control over cookie management. Our main objective is to analyze the legal classifications of browser cookies and evaluate their accessibility and comprehensibility to users. The analysis reveals significant variations in how different websites classify cookies, the cookie management available in different browsers and the level of user understanding of these categories. The research underscores the need for clearer communication and better education on cookie usage to enhance user awareness and consent. Our aim is to contribute to discussions on making cookie management practices in Ireland more transparent and user-friendly.**

***Index Terms*—Cookies, GDPR, Privacy, User Consent, cookie categories**

I. Introduction

The usage of cookies, which are little text files that websites install on users' devices to track user behavior for targeted advertising, has increased dramatically in the digital era. Cookies can be used to improve user experience and track user behavior. A cookie is sent from the server to the user's browser when they visit a website, and the browser saves the cookie. On subsequent visits, the browser sends the cookie back to the server, enabling the website to retrieve stored information about the user, such as login credentials or preferences. This approach is essential because web communication is based on the stateless HTTP protocol, which treats every request made by a browser to a server as a separate event with no memory of past interactions. Without the user's knowledge or consent, online businesses frequently sell or share aggregated cookie data with third parties for marketing, analytics, and other uses. The majority of users are not aware of how much data is tracked by cookies or how it is shared, used, and stored over time. Through cookies, malicious actors can follow past purchases to obtain credit card data or carry out other identity theft crimes. The GDPR requires websites to get users' explicit consent before setting up cookies that gather personal data on their devices. This consent needs to be explicit, unambiguous, given voluntarily, and informed. The high bar for valid permission set by the GDPR is not met by pre-checked boxes or implicit consent obtained through continuous surfing [1]. Existing research has shown that many cookie consent banners are designed in a way that nudges users towards accepting all cookies, rather than making a truly informed choice. Previous studies shows that many cookie consent banners employ ”dark patterns” that manipulate users into accepting all cookies, rather than making an informed choice. The authors argue this undermines the GDPR's consent principles and reduces user control over their data. [2]. In particular, our study aims at discussing the following research questions:

(1) What cookie management options are available in major web browsers and does it align with users' needs and expectations for privacy control and understanding?

(2) How do different sectors of Irish websites categorize and manage cookies, and which sectors demonstrate the greatest need for enhanced cookie compliance and user understanding?

Initially, we performed a survey to gauge users' understanding of cookies, their privacy concerns, and their management practices across different web browsers. The survey covered aspects such as familiarity with cookie types, the perceived risks of cookies, and preferences for cookie acceptance. While numerous studies have explored cookie usage and compliance with GDPR, there is a lack of specific focus on the Irish context. Our study uniquely contributes by providing a detailed analysis of cookie practices across various sectors in Ireland, highlighting compliance issues and sector-specific trends that have not been extensively documented. We analyzed a sample of Irish websites from various sectors, comparing their cookie usage against an established database to categorize the cookies according to updated research findings on user understanding. This analysis revealed sector-specific patterns in cookie deployment and highlighted areas where improved compliance measures are needed. Additionally, we examined the cookie management options offered by different web browsers to assess their efficacy in supporting user control over cookie preferences. The findings indicate notable disparities in cookie management practices across sectors and underscore the need for more intuitive consent mechanisms. By aligning cookie categories with user understanding and addressing privacy risks more effectively, our study aims to contribute to the development of better cookie compliance frameworks and enhance user awareness of privacy issues related to cookies. In the subsequent sections, we will detail our methodology, present the results of our analyses, and discuss the implications of our findings for users. Our goal is to offer actionable insights that can improve cookie consent practices and foster a more privacy-conscious online environment.

II. BACKGROUND AND RELATED WORK

A. Overview of GDPR

The General Data Protection Regulation (GDPR), which went into effect in May 2018 [1], marked a major change to the EU's data privacy regulations. Protecting personal data and ensuring that people have control over their information are the main goals of the GDPR. It requires users' explicit permission before their data may be processed or shared, mandating transparency in data collecting methods. This rule has a significant impact on web technology, especially as it relates to cookies.

1) Key Points of GDPR: Regardless of the organization's location, GDPR is applicable to all entities that process the sensitive information of individuals within the EU. This wide reach guarantees that any organization handling the data of EU people must abide by the rules. Any information that may be used to identify a living person is considered personal data, and this includes email addresses, names, location and contact information, and financial information. This wide definition includes a variety of data kinds that an organization might gather.

GDPR also gives several rights to people when it comes to the use of their personal data this includes:
Right to Access: This gives the individual the right to view their data.
Right to Rectification: Individuals can correct inaccurate or incomplete data.
Right to erasure: Also known as the "right to be forgotten," individuals can request data deletion under certain conditions.
Right to Object: Individuals can oppose the use of their data in specific circumstances.

In Ireland, the Data Protection Act 2018 [15] and the General Data Protection Regulation (GDPR) require organizations to have a valid legal basis before processing personal data. These bases include getting individuals' explicit agreement, which needs to be freely submitted, accurate, informed, and reversible, according to the Data Protection Commission (DPC) in Ireland [3]. According to a 2020 Irish Computer Society survey, 85% of Irish organizations primarily depend on consent and contractual necessity as their legal justifications for processing data [4]. Another legal foundation comes from statutory requirements, like those imposed on tax compliance or in response to requests from public authorities. For example, the Revenue Commissioners process personal data following the Taxes Consolidation Act 1997 [4]. 70% of Irish businesses justify data processing with legitimate objectives, such as direct marketing and fraud protection, as long as these interests don't conflict with people's rights [5]. Data processing may take place for duties performed in the public interest or under official authority, or to safeguard an individual's essential interests in an emergency [6].
If a breach of personal data puts people's rights and freedoms in danger, organizations must notify the appropriate authorities and the impacted parties as soon as possible [7]. The Data Protection Commission (DPC) in Ireland reports that 6,628 data breach notifications were made in 2020 alone, underscoring the vital need for prompt reporting [5]. Strong data breach response plans are essential, as the DPC stresses that missing this deadline for reporting might result in severe penalties. Organizations must put the necessary organizational and technical safeguards in place to ensure compliance with the GDPR, which strongly emphasizes responsibility as mentioned in [4]. This entails keeping records of processing operations and, if required, doing Data Protection Impact Assessments (DPIAs). To reduce potential risks related to data processing activities, 72% of firms had performed DPIAs, according to the Data Protection Commission's 2020 Annual Report. Additionally, to help enterprises meet their accountability requirements and ensure that data protection principles are ingrained in their operational procedures, the European Data Protection Board (EDPB) offers comprehensive guidance.

- **Consent:** Users must be informed about the use of cookies and must provide explicit consent before any cookies can be placed on their device.
- **Transparency** Websites must clearly explain the purpose of each cookie and how the collected data will be used.
- **User Rights:** Users have the right to access their data, request its deletion, and withdraw consent at any time.

B. Role of Cookies in Web Browsing

Browser Cookies allow websites to remember user preferences, preserve session information, and personalize content, all of which contribute to an improved online browsing experience. Cookies play a variety of technical and functional purposes when you browse the web. Some of the Technical cookie functions for different browsers are as follows:

- **Session Management:** For websites to manage user sessions, cookies are necessary. They contribute to the continuity of a user's surfing experience by temporarily saving data, like shopping cart contents and login passwords. Session cookies, for instance, save users' login information so they don't have to enter it again while navigating between pages on a website.
- **Data Storage:** Cookies let the server access small pieces of data from them when a user returns. User preferences, language settings, and other customized features may be included in this data. By allowing websites to remember users between sessions, persistent cookies that stay on the user's device for a certain amount of time improve the overall surfing experience.

- **Authentication:** Cookies are frequently used in authentication processes. By storing data that confirms a user's identity, authentication cookies provide safe access to website sections that are prohibited. For services that need user logins, like online banking or e-commerce platforms, this feature is essential because safe access is critical.
- **Security Features:** The Secure and HttpOnly flags are two examples of security features that come with some cookies. Because client-side scripts cannot access HttpOnly cookies, there is less chance of cross-site scripting (XSS) attacks. Only HTTPS is used to send secure cookies, guaranteeing that the data is secured throughout transit and preventing user information from being intercepted.

C. Consent Mechanism

Web technologies' consent procedures have significantly changed in response to growing regulatory scrutiny and user expectations around data protection. A consent mechanism in web technology is the procedures and instruments used to secure, handle, and retain user consent for purposes of collecting and processing data, especially when adhering to data protection laws such as the California Consumer Privacy Act (CCPA) [16] and the General Data Protection Regulation (GDPR). The main types of consent are - Explicit Content and Implied content. Explicit consent must be given through an express statement, leaving no room for misinterpretation. It should specify the data being processed, the purposes of processing, and any potential risks involved. According to Article 9(2)(a) of the GDPR, processing some types of personal data, like health data, requires specific consent. Additionally, compliance with Article 4(11) of the GDPR's formal definition of consent is mandated [8]. Implied consent is being harshly criticized, but this is predicated on the idea that people's ongoing internet use constitutes a type of required consent for accessing their personal information. According to GDPR, this approach is seen as inadequate since it does not guarantee that users are properly informed or have given their real agreement for the data practices. In situations when data processing is a standard component of a service and consumers are notified through terms and conditions, implied consent may be appropriate. But under GDPR, this strategy is being examined more closely, especially with regard to sensitive data categories.

D. Challenges in Cookie Consent Compliance

Many organisations, particularly small and medium-sized enterprises (SMEs), find it difficult to comply with the GDPR's complicated regulations. The rule requires major adjustments to a number of organizational procedures, yet many SMEs lack the means or know-how to properly handle compliance. Due to this, there is a significant chance of non-compliance and possible fines of up to 4% of worldwide turnover or €20 million, whichever is larger [9]. Numerous cookie consent procedures do not comply with GDPR regulations, according to studies. Pre-checked boxes, ambiguous wording in consent requests, and a dearth of obvious ways for users to modify their consent preferences are among the problems. A fundamental component of GDPR, informed consent, is undermined by these actions. On a German website, the researchers ran three tests with a total of 80000 unique users to examine the effects of notification position, choice type, and content framing on user consent behavior. They collected a substantial amount of information about how users interacted with consent notices in practical scenarios using their empirical technique. Users find it difficult to comprehend what they are consenting to when cookie categories are branded inconsistently across websites using ambiguous or technical phrases like ”Necessary”, ”Functional”, and ”Performance”. Many banners only offer the binary choices of ”Accept All” or ”Reject All”, preventing users from giving their specific agreement to any other kind of cookie use. Users are unable to make meaningful choices because of this. [10]

E. Enhancing User Understanding of Cookie Consent

According to the study [11], users frequently mix up the terms ”strictly necessary” and ”functional” cookies, in particular. This ambiguity indicates that, in order to improve user comprehension, these categories need to be redefined or distinguished more clearly. Websites should simplify the language used in consent banners, minimizing legal language and technical terms in order to increase user understanding of cookie consent. Information overload can be avoided by putting in place a structured information strategy, in which key details are provided up front along with links to more thorough explanations. Information about consent can be made more interesting and accessible by using visual aids like infographics and icons. Transparency and uniformity across websites can be improved by standardizing cookie categories and offering thorough descriptions for each type. Contextual consent requests, granular control over cookie preferences, and user-centric permission management platforms can all empower consumers and promote greater trust in online privacy policies.

III. Research Methodology

A. Analysis of cookie management in Major Browsers:

We compared the features of browser cookie management in order to comprehend how various browsers handle cookies and how this affects user privacy and consent. The purpose of this investigation was to assess how well major browsers handle cookies both technically and functionally.

1) Browser Selection: We selected a representative sample of popular web browsers for this analysis, including:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari
- Brave

2) Criteria for Analysis: The analysis is focused on the following criteria:

- Session Management: How each browser handles session cookies, including retention and deletion practices.
- Data Storage: The approach to persistent cookies, including expiration dates and storage capacity.
- Authentication: Support for Secure and HttpOnly attributes, and their impact on secure access.
- Security Features: Implementation of security features like SameSite attributes, Enhanced Tracking Protection (ETP), and Intelligent Tracking Prevention (ITP).

B. Survey

To complement the technical data on cookies, we conducted a survey to understand public awareness and the perceived need for education regarding cookie functions. This section outlines the survey design, implementation, and analysis. The survey was designed to find out the amount that the general public knew about cookies as well as whether they were interested to learn more. In total, there were 10 questions with multiple-choice responses. The survey was conducted online using Google Forms over a two-week period over a small population. Participants were asked questions about their current knowledge of cookies, their ability to identify different types of cookies, and their interest in further education on the topic. A complete list of questions asked in the survey can be found in Appendix A.

C. Analysis of Cookie categories in Irish Websites on different Sectors

The data collection phase was essential in our research, enabling us to gather comprehensive information about the cookies used by various Irish websites.

1) Web Scraping: We used Selenium to automate website access and cookie data extraction. A CSV file of websites, categorized by sector, was loaded into a pandas Data Frame and converted into a dictionary. The number of sites per sector is shown in table I.

Using Selenium's Options class, we set up the Chrome WebDriver in headless mode for efficiency and used ChromeDriverManager to ensure we always had the latest version. The WebDriver visited each website and downloaded all available cookies. To maintain uniformity, each cookie's domain was standardized to start with "www." and the website URL was appended to the cookie contents.

- **Cookie Names:** Specific identifiers for each cookie.
- **Cookie Purposes:** Descriptions of what each cookie does (e.g., tracking, authentication, personalization).
- **Cookie Lifespans:** Duration for which the cookies remain on the user's device.
- **Third-Party Involvement:** Identification of cookies set by third-party services.

TABLE I: Number of sites by category

Category	**Number of Sites**
Education	240
E-commerce	214
Sports	198
Media	196
Fashion	183
Charities & Nonprofits	162
Food & Beverage	148
Technology	135
Art & Culture	133
Utilities	130
Real Estate	113
Travel	110
Healthcare	106
Legal & Professional Services	99
Grocery	99
Government Agencies	92
Insurance	74
Automotive	54
Gaming	30
Music	5

D. Data Categorization

A crucial part of our analysis was classifying the data, which helped us arrange and make sense of the wide variety of cookies that Irish websites employ. We used an extensive dataset from the Open Cookie Database [13] and other relevant sources for this purpose. Building upon traditional cookie categories, we incorporated a new categorization system as outlined in the paper "Crumbling Cookie Categories: Deconstructing Common Cookie Categories to Create Categories that People Understand" [12]. This system provides clearer, more user-friendly categories, enhancing transparency and understanding. The new categories include:
Performance Cookies: Collect information about how visitors use a website (e.g., which pages are visited most often).
Functional Cookies: Allow the website to remember choices you make (e.g., your username, language, or the region you are in).
Advertising Cookies: utilized to provide advertisements that are more appropriate for you and your interests.
Security Cookies: Enhance security measures, such as protecting against CSRF attacks.
Anonymous Cookies: Do not collect personal data but track generic behavior.

Each cookie from our dataset was mapped to the corresponding category in the open cookie database [13], which included the following types:
Anonymous: 1241 cookies
Functional: 541 cookies
Performance: 462 cookies
Advertising: 267 cookies
Security: 10 cookies

IV. Results and Discussion

A. Analysis of cookie functions in different Browsers

The comparison of cookie functions and management across major web browsers reveals several key insights into their respective privacy and usability features. Browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge provide robust options for managing session and persistent cookies, including the ability to block third-party cookies and use private browsing modes. This flexibility allows users to tailor their browsing experience according to their privacy preferences. In contrast, Safari and Brave adopt a more restrictive approach. Safari utilizes Intelligent Tracking Prevention (ITP) to limit the lifespan of cookies and restrict cross-site tracking, while Brave blocks third-party cookies by default and incorporates additional privacy features like Tor integration for enhanced anonymity. Despite all browsers supporting essential security measures, such as Secure and HttpOnly attributes, Safari and Brave offer additional privacy-focused mechanisms that impact cookie functionality and tracking prevention. Overall, the choice of browser can significantly affect user privacy and convenience, with Safari and Brave prioritizing privacy at the expense of some flexibility, while Chrome, Firefox, and Edge provide more customizable options for cookie management. More details are provided in table II and III.

B. Survey

Our survey involved 60 participants and aimed to assess public awareness and attitudes toward cookie control in web browsers. The results indicated a predominantly positive response regarding cookies management. Notably, many participants, despite having used web browsers extensively, were not well-versed in the nuances of cookie control. We recognize that the results might not be entirely representative of the larger population given the comparatively small sample size of 60 people. Although the encouraging comments are encouraging, the small sample size prevents us from extrapolating the findings to a wider population. We anticipate that a larger sample size would likely provide a more comprehensive understanding of public attitudes and knowledge about cookies. The results:

1) *Browser Usage:* Google Chrome is the most popular browser among respondents 90%

2) *Understanding of Cookies:* 53.3% of respondents have limited or no understanding of cookies. Only 10% fully understand about the cookies and their usage.

3) *Concerns about privacy:* A significant majority of respondents 71.7% believe that cookies can compromise online privacy, reflecting a strong concern for data security and 41.7% are somewhat concerned, and 11.7%are very concerned.

4) *Interests in learning more about the cookies:* A large majority 78.3% are interested in learning more about cookies and online privacy, indicating a high level of curiosity and concern among users.

This survey provides valuable insights and suggests that there is an opportunity to enhance cookie management awareness among web browser users. More insights and details can be found in the table IV of appendix A

C. Analysis of Cookie data collected from Irish Websites:

1) *Top cookie types :* According to the analysis, functional cookies are most common, suggesting a strong reliance on user administration and site operations. Performance, analytics, and advertising cookies are also important for tracking and marketing. The table V reveals that the most frequently used cookies are primarily associated with Google Analytics (ga, gid), highlighting its extensive use for performance tracking. OneTrust’s ’OptanonConsent’ is also prominent, indicating a strong focus on managing cookie consent. Cookies are categorized into performance tracking, essential site functionality, and advertising, with cookies like ’fbp’ and ’gclau’ used for targeted marketing. Data controllers such as Google, OneTrust, Facebook, and Amazon Web Services play significant roles, with Google and OneTrust leading in analytics and consent management respectively, while Facebook and AWS contribute to advertising and session management. The high frequency of these cookies underscores their critical role in web performance, user compliance, and targeted marketing strategies.

2) *Distribution of cookie categories: :* The distribution of cookie categories is displayed in the fig.1 . The categories with the largest counts are ”Anonymous,” ”Functional,” ”Analytics,” ”Marketing,” and ”Security.” This indicates that the majority of cookies are either functional or anonymous. The fact that the ”Security” category has the lowest count indicates that less security cookies are being used by websites.

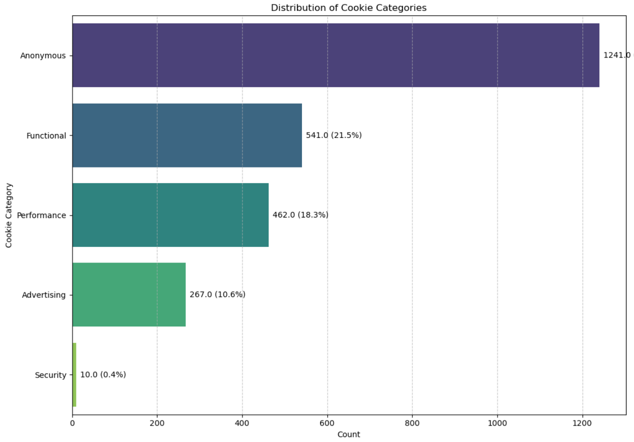

Fig. 1: Distribution of Cookie Categories

3) *Prevalence of Secure and HttpOnly cookies across different websites: :*

- **Secure Cookie:** The heatmap Fig.2, with counts of 83, 64, and 66, respectively, shows that the fashion, technology, and e-commerce sectors place a high priority on secure cookies. These high figures show a strong dedication to user data security, especially in sectors where handling of financial and personal data occurs often. Secure cookies are also notably prevalent in the media industry (62), indicating a focus on user data and content protection, likely to preserve intellectual property and provide secure content delivery. On the other hand, the Art & Culture category has eleven secure cookies, while the Music category has none, suggesting that strict security measures may not be as important to them. This might be as a result of the content's nature or the perception that certain categories carry less danger.

- **HttpOnly Cookie:** With counts of 52 and 42, respectively, the Education and E-commerce categories have the highest usage of HttpOnly cookies, which are essential for safeguarding session data by prohibiting client-side script access. This shows how critical it is to protect user session data, which is especially crucial for stopping cross-site scripting (XSS) attacks and guaranteeing safe user authentication. A substantial amount of HttpOnly cookies are also visible in the Sports and Utilities categories, indicating an emphasis on subscription and personal data security. On the other hand, the categories of Media (9 HttpOnly cookies) and Music (3 HttpOnly cookies) show less usage of this security precaution. This may indicate disparities in security objectives or difficulties in putting in place all-encompassing cookie security across these industries.The total variance in the use of HttpOnly cookies reveals different security requirements and methods, indicating that certain industries may want to improve their data security plans.

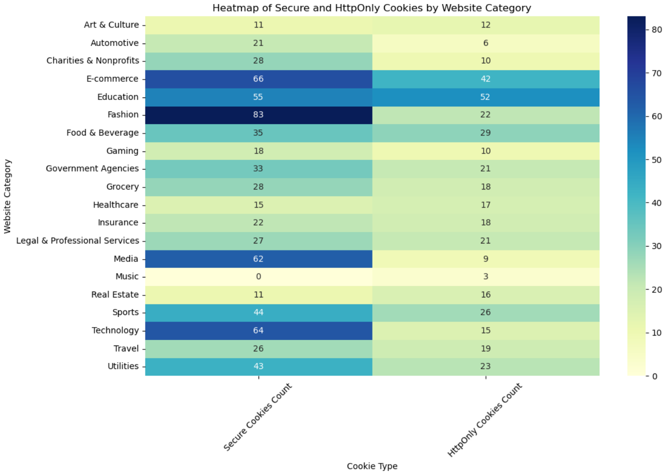

Fig. 2: Secure and HTTP Only cookie

4) Anonymous Cookies by Website Category: : Fig.3 shows Fashion (133 cookies), E-commerce (121 cookies), and Media (117 cookies) categories have the highest number of anonymous cookies. This suggests these industries may prioritize user tracking and analytics without identifying individuals, possibly due to a high focus on personalized advertising and content recommendation. Education (112 cookies) and Technology (88 cookies) also feature a significant number of anonymous cookies. In education, anonymous cookies might be used to track user engagement with educational content, while technology websites might use them for user behavior analytics and feature personalization.

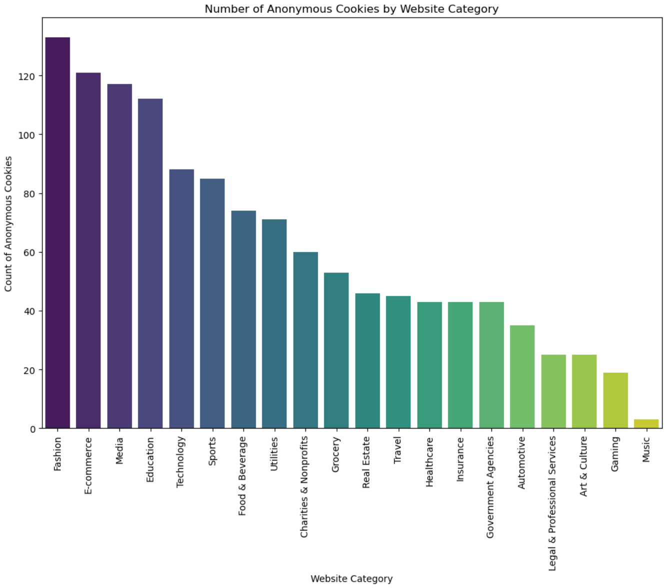

Fig. 3: Number of Anonymous cookie by website category

Our analysis revealed that 68% of Irish websites use tracking cookies, with a notable 25% employing third-party cookies. Particularly concerning is the use of third-party cookies on 45% of government websites, suggesting a gap in public sector compliance with GDPR.

V. Conclusion and Future study

This research looks closely at how cookies are used on Irish websites, focusing on GDPR compliance, privacy issues, and user awareness. We found differences in how various web browsers handle cookies. For instance, privacy-focused browsers like Safari and Brave offer stricter controls compared to others. Despite growing concern about online privacy, many users still lack a clear understanding of cookies and their purposes, which points to the need for better transparency and education. While sectors such as fashion, technology, and e-commerce are doing well in protecting user data, the infrequent use of security cookies suggests there's room for improvement. The inconsistencies in how cookies are categorized and how consent is managed also make it harder to follow GDPR rules, highlighting the need for clearer and more consistent consent processes. To enhance GDPR compliance, we recommend that websites standardize their use of cookie banners to provide clearer consent options. Additionally, browser developers should implement features such as automatic deletion of non-essential cookies and more transparent privacy settings to empower users in managing their online data footprint. Additionally, enhancing browser features for managing cookies could better support user privacy. Specific strategies for different industries should be created to tackle unique compliance challenges. Long-term studies should track how changes impact user behavior, website practices, and adherence to regulations. While this study provides valuable insights, it is limited to Irish websites and may not fully capture the complexities of cookie usage in other regions. Future research may explore similar analyses in different geographical contexts and examine the long-term effects of evolving digital privacy regulations on user behavior and website compliance. As digital landscapes continue to evolve, it is imperative that both regulatory frameworks and technological solutions adapt accordingly. By enhancing transparency and user control over data, we can create a more secure and trustworthy online environment. This study serves as a call to action for all stakeholders to prioritize privacy and compliance in their digital strategies.

References

[1] GDPR.EU, ”General Data Protection Regulation (GDPR),” 2018. [Online]. Available: https://gdpr.eu/tag/gdpr/.

[2] D. W. Woods and R. Böhme, ”The commodification of consent,” Computers Security, vol. 115, p. 102605, 2022.[Online]. Available: https://doi.org/10.1016/j.cose.2022.102605

[3] Data Protection Commission, “Guidance Note: Legal Bases for Processing Personal Data,” 2019. [Online]. Available: https://www.dataprotection.ie/en/legal-bases-processing-personal-data

[4] Irish Computer Society, “Irish Computer Society: Data Protection Survey,” 2020. [Online]. Available: https://www.ics.ie/news/data-protection-survey-2020

[5] Office of the Revenue Commissioners, “Taxes Consolidation Act 1997,” 1997. [Online]. Available: https://www.revenue.ie/en/tax-professionals/legislation/taxes-consolidation-act-1997/index.aspx

[6] Data Protection Commission, “Annual Report 2020,” 2021. [Online]. Available: https://www.dataprotection.ie/en/dpc-annual-report-2020

[7] Government of Ireland, “Data Protection Act 2018, Sections 40–44,” 2018. [Online]. Available: https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

[8] European Parliament and Council of the European Union, ”General Data Protection Regulation (GDPR), Article 33,” 2016.

[9] ”Explicit Consent,” Health Research Board, Jul. 23, 2024. [Online]. Available: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/consent/explicit-consent/

[10] ”Data Protection Presents Ongoing Challenges for Irish Institutions,” Education Magazine, Aug. 23, 2021. [Online]. Available: https://educationmagazine.ie/2021/08/23/data-protection-presents-ongoing-challenges-for-irish-institutions/

[11] C. Utz, F. Schaub, M. Degeling, S. Fahl, and T. Holz, ”(Un)informed Consent: Studying GDPR Consent Notices in the Field,” in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS ’19)*, London, United Kingdom, 2019, pp. 973-990.

[12] S. Jiwani, R. Sasheendran, A. Abhyankar, E. Bouma-Sims, and L. F. Cranor, ”Crumbling Cookie Categories: Deconstructing Common Cookie Categories to Create Categories that People Understand,” Proc. Priv. Enhancing Technol., 2024.

[13] J. Kwakman, ”Open Cookie Database,” GitHub repository, [Online]. Available: https://github.com/jkwakman/Open-Cookie-Database

[14] M.D.C. Freitas and M. Mira da Silva, ”GDPR Compliance in SMEs: There is much to be done,”Journal of Information Systems Engineering Management, vol.3, no.4, p.30, 2018.

[15] Law Reform Commission, ”European Union (Withdrawal) Act 2018,” Revised Acts, 2018. [Online]. Available: https://revisedacts.lawreform.ie/eli/2018/act/7/revised/en/html

[16] Office of the California Attorney General, ”California Consumer Privacy Act of 2018,” June 2018. [Online]. Available: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[17] Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., and Holz, T. (2019) ’We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR’s Impact on Web Privacy’, Proceedings of the 2019 Network and Distributed System Security Symposium, Internet Society.[Online] Available: http://dx.doi.org/10.14722/ndss.2019.23378

[18] Pantelic, O., Jovic, K., and Krstovic, S. (2022) ’Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations’, Sustainability, 14(9), p. 5015. [Online] Available: https://doi.org/10.3390/su14095015

[19] Linn, J. (2005) ’Technology and web user data privacy - a survey of risks and countermeasures’, IEEE Security Privacy, 3(1), pp. 52-58. doi: 10.1109/MSP.2005.27.[Online] Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1392701&isnumber=30310.

[20] Park, J. S. and Sandhu, R. (2000) ’Secure cookies on the Web’, IEEE Internet Computing, 4(4), pp. 36-44. doi: 10.1109/4236.865085.[Online] Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=865085

[21] S. Singh, et al., ”Enhancing Cookie Functionality for Secure and Privacy-Preserving Web Interactions,” 2021.

[22] R. Martinez, et al., ”Enhancing Cookie Management Through User-Centric Design: A Case Study,” 2023.

APPENDIX

A.1 TABLES

TABLE II: Comparison of Cookie Functions Across Major Browsers

Cookie Function	Browser	Technical Function Explanation
Session Management	Google Chrome	Retains session cookies until exit; can clear cookies on exit.
	Mozilla Firefox	Retains session cookies; options to clear cookies on exit.
	Microsoft Edge	Similar to Chrome; user options to clear cookies on exit.
	Safari	Aggressively clears session cookies; ITP impacts lifespan.
	Brave	Blocks third-party cookies by default; session cookies managed with privacy focus.
Data Storage	Google Chrome	Generous; persistent cookies retained based on expiration dates.
	Mozilla Firefox	Extensive; managed through privacy settings.
	Microsoft Edge	Similar to Chrome; based on expiration dates.
	Safari	Restricted by ITP; limited lifespan for persistent cookies.
	Brave	Privacy-focused; third-party cookies blocked; persistent cookies managed with restrictions.
Authentication	Google Chrome	Supports Secure and HttpOnly attributes; enforced for secure connections.
	Mozilla Firefox	Supports Secure and HttpOnly attributes; configurable through privacy settings.
	Microsoft Edge	Supports Secure and HttpOnly attributes; similar to Chrome.
	Safari	Supports Secure and HttpOnly attributes; ITP may affect functionality.
	Brave	Supports Secure and HttpOnly attributes; additional privacy protections applied.
Security Features	Google Chrome	Enforces SameSite attributes; blocks third-party cookies as per user settings.
	Mozilla Firefox	Supports SameSite attributes; Enhanced Tracking Protection (ETP) blocks cookies from known trackers.
	Microsoft Edge	Supports SameSite attributes; privacy controls to manage cookies.
	Safari	Implements ITP; restricts cross-site tracking and cookie usage.
	Brave	Blocks third-party cookies by default; supports SameSite attributes; enhanced privacy focus.

TABLE III: Browser Cookie Management

Browser	Types of Cookies Contained	Third-Party Cookies	Cookie Management Options
Google Chrome	Session Cookies, Persistent Cookies, SameSite Cookies	Yes	Allows blocking of third-party cookies, site-specific cookie management, incognito mode for cookie-free browsing
Mozilla Firefox	Session Cookies, Persistent Cookies, SameSite Cookies	Yes	Enhanced Tracking Protection, cookie blocking, site-specific cookie management, private browsing mode
Microsoft Edge	Session Cookies, Persistent Cookies, SameSite Cookies	Yes	Tracking prevention options, cookie blocking, site-specific cookie management, InPrivate browsing mode
Safari	Session Cookies, Persistent Cookies, SameSite Cookies	No	Intelligent Tracking Prevention (ITP), site-specific cookie management, private browsing mode
Brave	Session Cookies, Persistent Cookies, SameSite Cookies	No	Built-in cookie blocking, site-specific cookie management, private browsing with Tor

TABLE IV: Survey Analysis

Category	**Details**
Popular Browsers	Chrome: 90%, Firefox: 23.3%, Safari: 31.7%, Edge: 30%, Opera: 15%, Brave: 25%, All: 5%
Understanding of Cookies	Yes: 10%, Somewhat: 36.7%, No: 53.3%
Clearing Cookies/Cache	Daily: 8.3%, Weekly: 10%, Frequently: 30%, Rarely: 35%, Never: 16.7%
Privacy Concerns	Yes: 71.7%, No: 6.7%, Maybe: 21.7%
Concern Level	Very concerned: 11.7%, Somewhat concerned: 41.7%, Neutral: 45%, Not very concerned: 1%
Personalized Content	Very important: 15%, Somewhat important: 16.7%, Neutral: 35%, Not very important: 30%
Familiarity with Cookies	Session: 65%, Persistent: 31.7%, Third Party: 71.7%, Secure: 46.7%
Most Acceptable Cookies	Necessary: 80%, Preference: 56.7%, Statistical: 15%
Least Acceptable Cookies	Marketing: 55%, Third-party: 46.7%, Statistical: 35%
Interest in Learning More	Yes: 78.3%, No: 5%, Maybe: 16.7%

TABLE V: Top 10 Cookies by Frequency with Categories, Data Controllers, and Platforms

Name	**Category**	**Data Controller**	**Platform**	**Counts**
_ga	Performance	Google	Google Analytics	138
OptanonConsent	Functional	OneTrust	OneTrust	91
_gid	Performance	Google	Google Analytics	68
_fbp	Advertising	Facebook	Facebook	55
_gcl_au	Advertising	Google	Google	49
PHPSESSID	Functional	PHP.net	PHP.net	30
ASP.NET_SessionId	Functional	Microsoft	ASP.net	25
__cf_bm	Functional	Cloudflare	Cloudflare	24
AWSALB	Functional	Amazon Web Services	Amazon Web Services	22
AWSALBCORS	Functional	Amazon Web Services	Amazon Web Services	21

A.2 Survey Questions

1) Which web browsers do you use regularly? (Check all that apply)
   - □ Google Chrome
   - □ Mozilla Firefox
   - □ Safari
   - □ Microsoft Edge
   - □ Opera
   - □ Brave
   - □ All of the above
2) Do you understand what cookies are and how they are used by websites?
   - ○ Yes, completely
   - ○ Somewhat
   - ○ No, not really
3) How often do you clear your browser cookies/cache?
   - ○ Daily
   - ○ Weekly
   - ○ Frequently
   - ○ Rarely
   - ○ Never
4) Do you believe cookies can compromise your online privacy?
   - ○ Yes
   - ○ No
   - ○ Maybe
5) How concerned are you about your online privacy regarding the use of cookies by websites?
   - ○ Very concerned
   - ○ Somewhat concerned
   - ○ Neutral
   - ○ Not very concerned
   - ○ Not concerned at all
6) When browsing websites, how important is it for you to have personalized content based on your browsing history or preferences?
   - ○ Very important
   - ○ Somewhat important
   - ○ Neutral
   - ○ Not very important
   - ○ Not important at all
7) Which of the following types of cookies are you familiar with? (Check all that apply)
   - □ Session Cookies
   - □ Persistent Cookies
   - □ Third Party Cookies
   - □ Secure Cookies
   - □ Http Cookies
8) Which type of cookies do you find most acceptable when browsing websites? (Check all that apply)
   - □ Necessary cookies (essential for website functionality)
   - □ Preference cookies (store user preferences)
   - □ Statistical cookies (track website usage for analytics)
   - □ Marketing cookies (targeted advertising)
   - □ Third-party cookies (used by third-party services embedded in the website)
   - □ I don't know/I'm not sure
9) Which type of cookies do you find least acceptable when browsing websites? (Check all that apply)
   - □ Necessary cookies (essential for website functionality)
   - □ Preference cookies (store user preferences)
   - □ Statistical cookies (track website usage for analytics)
   - □ Marketing cookies (targeted advertising)
   - □ Third-party cookies (used by third-party services embedded in the website)
   - □ I don't know/I'm not sure
10) Would you like to learn more about cookies and online privacy?
    - ○ Yes
    - ○ No
    - ○ Maybe
11) Do you have any additional comments or concerns about the use of cookies on websites?