Usability and User Experience, Vol. 194, 2025, 293–303
https://doi.org/10.54941/ahfe1006692

Design Principles for Cookie Banners: Balancing Legal Compliance and Usability

Maria Rigou and Niki Georgiadou

Department of Management Science and Technology, University of Patras, Koukouli,
GR 26334, Greece

ABSTRACT

Ever since the GDPR and the related legal framework came into force, web users come across and interact with cookie banners extremely often while navigating. These short but numerous interactions sum up to a considerable effort, which becomes even bigger when cookie banners are poorly designed or deliberately try to deceive users in giving full consent. This article investigates the issue of cookie banner design, considering both the legal and the usability requirements that should be respected to allow users adequate control over their data while browsing the web. It also critically examines widely used design patterns for cookie banners in terms of GDPR and usability compliance and provides a set of cookie banner design guidelines, emphasizing the importance of balancing transparency, simplicity, and control in banner design while avoiding dark patterns and consent fatigue.

Keywords: GDPR, Cookie, Cookie banner, Privacy, Consent, Usability, Dark patterns

INTRODUCTION

Cookies have become an integral part of the online browsing experience. A cookie is a small text file that a website stores on a user's device to remember information about their past visits. These files allow websites to perform several functions, such as keeping users logged in, remembering their previously stated (or derived) preferences, collecting data to enhance website performance and user experience. However, due to their ability to track and store user data, cookies have raised significant privacy concerns along the years, particularly in the European context where a strict legal framework was imposed to set the rules for giving users control over their private data and the way websites collect, store and use these data.

Cookies were first introduced to allow e-shops to manage user shopping carts by remembering the contents as users navigated through different pages of a website. This functionality quickly expanded to include other uses, such as storing login details and user preferences for personalizing the delivered content. As the Internet grew, cookies evolved as well and expanded their functionality and purpose. In the late 1990s, third-party cookies were introduced, enabling advertisers to track users over several websites and build detailed profiles based on their browsing history (Chen et al., 2021). Based on their purpose, cookies can be broadly categorized into:

- **Strictly necessary cookies**, which support the core functionality of the website, such as shopping carts, session management, and user login.
- **Performance cookies** (also called analytics cookies), which collect information about how visitors use a website, such as the pages they visit most frequently and any problems they might encounter. They can be used to improve the website's overall performance and user experience.
- **Functional/personalization cookies** allow websites to remember user preferences and choices, such as language selection, time zone, login details or adjusted content (e.g. traffic information tailored to the current user location), to provide a more usable website.
- **Targeting/advertising cookies** are used to identify visitors between different websites, e.g. content partners, banner networks. Those cookies may be used by companies to build a profile of visitor interests or show relevant ads on other websites.

Depending on their domain of origin, cookies can be categorized as **first-party** or **third-party**. A third-party domain that hosts resources referenced by multiple websites can track users across all these sites, an approach deployed by advertising networks for cross-site tracking (Chen et al., 2021). Based on their lifespan cookies are distinguished as session cookies and persistent cookies. An example of persistent cookies are zombie cookies (also called evercookies or supercookies) which are stored in multiple places on the user's device, making them hard to remove. Currently, third-party cookies are the backbone of the most privacy intrusive practices, such as cookies synchronization, which allows data about user behaviour to be shared between websites. As a result, some web browsers already block third-party cookies by default, while other major browsers plan to do so shortly (Tomisek, 2023; Bohn, 2020). Yet, third – party cookies remain a part of the internet advertisement system and information about them is essential for the exercise of the users' fundamental right to protect their privacy and personal data. Relatively recent legal constraints have imposed restrictions on the anarchy caused by new and more privacy-invasive ways of tracking users through cookies and related mechanisms that had prevailed on the web, driven mainly by the online advertising industry. In Europe, the GDPR and the related legal framework puts specific prerequisites on the use of cookies and asks for informed user consent before storing cookies, a process implemented through cookie banners.

A cookie banner is a notification, often appearing at the top or bottom of a webpage, that informs users about the use of cookies on the site and seeks their consent to store and access certain types of cookies on their devices. The implementation of cookie banners is largely driven by the requirements set forth by the legal framework that is applicable in each case but should also comply with usability design guidelines to assure effective interaction for users and a high level of user experience. This article describes the key aspects of the legal framework for cookies in Europe with an emphasis on the functional specifications of cookie banners that can be practically applied to ensure legal compliance (section 2). In section 3, the topic of designing cookie banners is approached from the perspective of interaction design, introducing a set of guidelines for effective user interaction, protection of user rights to privacy and avoidance of dark patterns. Section 4 concludes and provides foreseen future directions.

EU COOKIES LEGISLATION

The main EU regulations for cookies are the Directive 2002/58/EC, known as the "e-Privacy Directive" and the General Data Protection Regulation (GDPR). Article 5(3) of e-Privacy Directive regulates the storing of information and the gaining of access to information that is already stored in the terminal equipment of users and subscribers. In its initial version, it provided for a system of subsequent objection by online users to the use of cookies (**opt-out**). In fact, the users had to be offered the right to refuse the use of cookies. With the Directive 2009/136/EC, the installation and use of cookies by website administrators became stricter, introducing a system of obtaining the prior consent of the user before processing (**opt-in**). In other words, a website should ask the visitor to authorize the storage and retrieval of data sent through cookies and similar tracking mechanisms before delivering and installing them (Lee, 2011; Tomisek, 2023; Trevisan et al., 2019).

As stated in article 5(3) of the Directive 2009/136/EC and article 94(2) of the GDPR, the consent requirement itself must be interpreted in accordance with the consent requirements of the GDPR (Tomisek; 2023, Santos et al., 2020; Judgement Planet49, par. 56). Generally, consent can only be an appropriate lawful basis if a data subject is offered control and a genuine choice regarding accepting or declining the terms without detriment (Naithani, 2024).

Furthermore, article 5(3) of Directive 2002/58/EC establishes two exceptions to the consent condition.

1. The use of cookies is necessary for "*the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network*". The same wording was used in the revised directive, but the words "*or facilitating*" were removed, which could be interpreted as a further indication that the European Legislator intended to restrict the perimeter of the exemption afforded by Article 5.3. The transmission of electronic communication would become impossible without the use of the cookie. Cookies that merely assist the communication are not covered (Naithani, 2024).
2. The installation and use of cookies is "*as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*". In this case, there must be a clear link between the strict necessity of a cookie and the delivery of the service explicitly requested by the user for the exemption to apply (Article 29 WP Opinion 4/2012).

The proposal of a Regulation on Privacy and Electronic Communications (European Commission, 2017), in comparison with the Directive 2002/58/EC, establishes a new exception to the consent condition and that is the collection of information from end user's terminal equipment, necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user (article 8(1d)). However, the web audience measurement ground should not be broadly interpreted as it could lead to a lower level of protection for user devices (EDPB, 2021).

CRITERIA OF LAWFUL CONSENT

The wording of Article 4(11) of GDPR requires a "*freely given, specific, informed and unambiguous*" indication of the data subject's wishes in the form of a statement or of "*clear affirmative action*" signifying agreement to the processing of the personal data relating to him or her (Judgement Planet49, par. 61). Thus, lawful consent clearly points to the following obligatory criteria:

a. Clear affirmative act. This requirement indicates an active, rather than passive, behaviour, "*such as a written or an oral statement… ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent*" (GDPR, recital 32). In practice, on several websites a visible notice regarding cookies collection can be found together with a link to the cookies' policy document (e.g. "*Our website uses cookies. By continuing we assume your permission to deploy cookies, as detailed in our privacy and cookies policy*"). Such practice does not comply with the GDPR. Websites are obligated to ensure that the user explicitly agrees with the use of cookies (Bachňáková Rózenfeldová & Sokol, 2018).

b. Freely given consent. This requirement suggests the user's free choice to accept or refuse the use of cookies. "*Freely given*" means the user must be offered real choice and control; if they are manipulated or feel compelled to agree to the processing of their personal data, this does not constitute valid consent (Degeling et al., 2019).

At first, websites often manipulate users into consenting to cookies through various deceptive design patterns (also known as "*dark patterns*") that mislead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data (Naithani, 2024). So, cookies' buttons must be equally weighted in terms of colour, size and placement. This means that the "*Accept button*" no longer may be more prominent or a different colour than the "*Reject button*". Cookie banner "*Accept*", and "*Rejec*t" buttons must have same colour, size and be placed in the first layer of the cookie banner next to each other. Another pattern is the missing reject-button. Many cookie banners include a "*settings*" button, which takes the user to the second layer of the cookie banner, where the reject button is a choice. This is a dark pattern, which introduces "*more clicks*" to reject cookies than accept. The regulation implies that the user must be able, with the same number of actions ("*clicks*") and from the same level, either to accept the use of trackers (those for which consent is required) or to reject all or each category of trackers separately. Of decisive importance is the ability of the user to withdraw his consent in the same way and with the same ease with which he declared it (Fich, 2022).

Secondly, cookie walls are an obstacle to valid consent, because they leave no space for a genuine, free choice. Consent cannot be enforced by preventing access to a website or mobile application if consent is not given (Tomisek, 2023). On the other hand, as stated in the proposed e-privacy regulation, access to a free service can be made conditional on accepting cookies, provided that the service provider offers an equivalent option that does not require the acceptance of cookies. This means websites can use cookie walls if they offer the user the choice for an alternative cookie-less service.

c. Specific consent. "*Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them*" (Recital 32 of GDPR). Cookie banners must include checkboxes in their design, so the user can choose to give consent to functional, statistic or marketing cookies. These checkboxes must be "*un-ticked*" as default. The need for specific consent in combination with the notion of purpose limitation in Article 5(1b) of GDPR functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data (Judgement Meta Platforms and Others, par. 109).

d. Informed consent. This requirement implies that the user must have previously been informed about the purposes of the processing, the data or categories of data concerned by the processing, the recipients or categories of recipients of the personal data, as well as the name, trade name and address of the social service provider of the information and any representative thereof. The text of the update should be easy to read regardless of the terminal device from which it is accessed (portable or stable device) (Naithani, 2024). The information must be clearly comprehensible and sufficiently detailed to enable the user to comprehend the functioning of the cookies employed (Judgement Planet49, par. 74). Opinion 15/2011 mandates the websites to offer the user a short resume of their cookie policy and a link to page containing all details (Degeling et al., 2019), while it is up to them to decide whether this will be inside the privacy policy section or as a separate cookie policy section. The cookie policy needs to be up to date (Pantelic et al., 2022).

e. Unambiguous consent. This provision can be described as an indisputable and objective expression of the user's acceptance with the use of cookies, strengthening the "*opt-in*" principle introduced in the Directive 2009/136/EC. The data subject must enjoy a high degree of autonomy when choosing whether to give consent (Santos et al., 2020). Consent cannot be based on inaction or silence but must be expressed actively, verbally or through other clear affirmative action indicating a deliberate declaration of intent. Thus, "*browser settings which would accept by default the targeting* *of the user (through the use of cookies)*" are not legitimate (Bachňáková Rózenfeldová & Sokol, 2018).

USABILITY CONSIDERATIONS FOR COOKIE BANNERS' DESIGN

Recent studies have explored the design and usability of cookie consent interfaces, highlighting the impact of various design elements on user behaviour and preferences. The main types of cookie banners from a design can be distinguished as *Implied Consent Banner, Notice-Only Banners, Opt-Out Banners, Full-Choice Banners (Explicit Consent), Layered or Granular Consent Banners* and *Pop-up/Modal Banners*. From a usability perspective, there are several considerations related to these types. Opt-out banners and pop-up banners are particularly problematic, as they often employ dark patterns or overly intrusive designs that frustrate users. Layered consent banners can also reduce usability due to complexity, leading to consent fatigue. Res-arch indicates that fully-blocking interfaces should be avoided, while persistent buttons for later changes are most effective (Hadid et al., 2020). Users prefer slider designs for ease of use and customizability (Singh et al., 2022) and the initial set of options displayed has the largest effect on user behaviour (Bouma-Sims et al., 2023). In fact, Mejtoft et al. (2023) argue that design, rather than trust in the organization, is crucial for users' decisions. Bright patterns highlighting decline options and behavioural levers significantly affect consent decisions and user satisfaction (Bielova et al., 2024).

Another issue is that cookie banners appear on different websites and in different designs thus taking users additional time and cognitive effort to read, understand, evaluate, and choose the preferred option on each website (Naithani, 2024; Bauer et al., 2021). The frequently posed requirement for consent can lead to user overload and fatigue (Naithani, 2024), a phenomenon referred to as "consent fatigue" (i.e. repeated exposure to cookie banners across different websites may cause users to automatically accept cookies without fully understanding their implications) (Borberg et al., 2022; Nouwens et al., 2020). People with high levels of privacy fatigue are more likely to "do nothing" in response to the misuse of their personal information (Choi et al., 2018).

Apart from physical endurance, judgement and decision-making also trigger psychological mechanisms (Coventry et al., 2016). Providing too much information upfront may overwhelm users, while too little information may jeopardise transparency requirements. Studies have observed that users see consent as inevitable while browsing and blindly agree to the terms (Rossi & Lenzini, 2020) and that cookie banner design has substantial impact on the privacy choices by users (Bauer et al., 2021). Examples include positioning of options, use of colours and visualizations, and formulation of instructions (Leonard et al., 2008). Furthermore, the choice architecture of the cookie banner could "nudge" users into sharing their data (Leonard et al., 2008) by manipulating users via dark patterns, such as predefined settings that need active steps to change, visual features steering users, complex language, hiding the 'reject cookies' button, etc. (Naithani, 2024).

To address these challenges, website owners must strike a balance between compliance and usability by designing cookie banners that are clear, concise, and easy to navigate, thereby fostering trust while adhering to regulatory requirements.

1. **Clarity and Simplicity**. The language used in cookie banners should be clear and concise, avoiding legal and technical jargon to ensure that users of all backgrounds can easily comprehend the information presented (Santos et al., 2021). It is also crucial to bear in mind that people will see (and even try to read) the consent text and options on a screen that may even be on a limited dimensions' smartphone, which imposes strict specifications on the way textual information should be formatted and how white space should be used to foster users reading and comprehension process (Miniukovich et al., 2017).
2. **Visibility and Accessibility**. The cookie banner must be easily visible and accessible when a user visits the website. It should not be hidden or obscured by other elements, such as ads or content. The placement of the banner should be prominent enough to catch the user's attention without being intrusive.
3. **Minimum Disruption**. While cookie banners need to be visible, they should also minimize disruption to the user experience. Banners should be designed to integrate smoothly with the website layout, allowing users to interact with the content while still making an informed choice about cookies (Habib et al., 2022). Pop-ups should be easy to close or dismiss without accidentally accepting cookies.
4. **Clear Options for Consent**. A cookie banner should present users with clear, distinct options to accept all cookies, deny all (which practically means to only allow the strictly necessary cookies), and an option to manage cookie settings for those users that are willing to customize which types of cookies they will accept (Tankala, 2023). These options should be equally prominent in terms of design, size, color, and placement (no additional clicks should be required to reach any of them). Consent must be an active choice as already discussed.
5. **Option to Not Make Any Consent Decision**. Users should be allowed to dismiss the banner without giving or denying consent to any cookies (Zachariah, 2024). In this case, it is important to remember that closing the cookie banner doesn't mean that they have accepted any cookies other than those that are exempted from the requirement of explicit.
6. **Clear Information on Data Usage**. The cookie banner should provide transparent information about what data is collected, how it will be used, who will have access to it, and how long it will be retained. This information should be easily accessible, typically through a "Learn more" link or an expandable section within the banner.
7. **Granular Consent Choices**. Where possible, cookie banners should offer granular choices, allowing users to opt in or out of different categories of cookies (e.g., strictly necessary, performance, functional, and marketing cookies) (Nouwens et al., 2020).

8. **No Dark Patterns.** Dark patterns, or manipulative design techniques intended to nudge users toward a particular decision (like accepting all cookies), should be avoided (Kocyigit et al., 2022; Mejtoft et al., 2021; Berens at al.,2022). This includes tactics like using colour contrasts to make the "accept" button more prominent than the "reject" button or making the rejection option more difficult to find (Mathur et al., 2019).
9. **Consistent Appearance Across Devices.** The cookie banner should be responsive and maintain a consistent appearance across all devices, including desktops, tablets, and smartphones. The layout should adjust to different screen sizes without sacrificing clarity or functionality (Web Content Accessibility Guidelines (WCAG) 2.1).
10. **Easy Access to Change Preferences.** Users should be able to easily change their cookie preferences at any time. The process for modifying consent should be straightforward, allowing users to withdraw consent as easily as it was given. Users should not be asked repeatedly to give their consent for cookies they have rejected in the past, nor should they be asked to give consent more than once during the same session.
11. **Timely Reminders and Updates.** Regular reminders or notifications to review cookie preferences can be a good practice, especially when there are changes to the types of cookies used or to privacy policies. However, these reminders should not be too frequent or repetitive, as they could negatively impact the user experience.

Conforming to these guidelines still does not guarantee a positive user experience without thorough user testing. Also, designers should consider the "*privacy paradox*" phenomenon; in surveys, people say they care about privacy, but they often divulge personal data in exchange for minimal benefits or convenience, and very few uses technical tools to protect their privacy online (Borgesius et al., 2017). Yet, privacy is a fundamental issue for those involved in human–computer interaction and should be protected by adopting a privacy-by-design approach within legal boundaries (Coventry et al., 2016).

CONCLUSION

Depending on the types of information, they collect and the method they use, cookies may be a legitimate and useful means of optimizing service delivery in the information society, but they may also constitute an arbitrary invasion in the private sphere of online users through tracking and profiling. The implementation of the e-Privacy Directive, the GDPR, and the proposal of the e-Privacy Regulation that will repeal the Directive harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities while using cookies. However, the design of cookie banners is not described in any regulation, although this issue has substantial impact on the privacy choices by users. In this article we approach the issue of cookie banner design considering both the legal and the usability requirements that should be respected to allow the users adequate control over their data while browsing the web. We conclude a set of usability design guidelines for cookie banners that may be used to guide their implementation.

REFERENCES

Bauer, Jan M., Regitze Bergstrøm, and Rune Foss-Madsen. "Are you sure, you want a cookie?–The effects of choice architecture on users' decisions about sharing private online data." *Computers in Human behavior* 120 (2021). https://doi.org/10.1016/j.chb.2021.106729

Bachňáková Rózenfeldová, Laura & Sokol, Pavol. (2018). New Initiatives and Approaches in the Law of Cookies in the EU.

Berens, Benjamin Maximilian, Heike Dietmann, Chiara Krisam, Oksana Kulyk, and Melanie Volkamer. "Cookie disclaimers: Impact of design and users' attitude." *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–20. 2022.

Bielova, Nataliia, Laura Litvine, Anysia Nguyen, Mariam Chammat, Vincent Toubiana, and Estelle Hary. The effect of design patterns on (Present and Future) cookie consent decisions. In: *33rd USENIX Security Symposium (USENIX Security 24)*. 2024. p. 2813–2830.

Bohn, Dieter. "Google to 'phase out' third-party cookies in Chrome, but not for two years". 2020. Available at: https://www.theverge.com/2020/1/14/21064698/google-third-party-cookies-chrome-two-years-privacy-safari-firefox (20.11.2024).

Borberg, Ida Marie, Rene Hougaard, Willard Rafnsson, and Oksana Kulyk. "'So I Sold My Soul': Effects of Dark Patterns in Cookie Notices on End -User Behavior and Perceptions." In *Proceedings 2022 Symposium on Usable Security*. Internet Society, 2022. https://doi.org/10.14722/usec.2022.23026

Borgesius, Zuiderveen, Frederik J., Sanne Kruikemeier, Sophie C. Boerman, and Natali Helberger. "Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the ePrivacy Regulation." *Eur. Data Prot. L. Rev.* 3, 353–368. 2017.

Bouma-Sims, Elijah Robert, Megan Li, Yanzi Lin, Adia Sakura-Lemessy, Alexandra Nisenoff, Ellie Young, Eleanor Birrell, Lorrie Faith Cranor, and Hana Habib. "A US-UK Usability Evaluation of Consent Management Platform Cookie Con Sent Interface Design on Desktop and Mobile." In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 68:1–36. ACM, 2023. https://doi.org/10.1145/3544548.3580725

Chen, Quan, Panagiotis Ilia, Michalis Polychronakis, and Alexandros Kapravelos. "Cookie Swap Party: Abusing First-Party Cookies for Web Tracking." In *Proceedings of the Web Conference 2021*, 2117–29. WWW '21. New York, NY, USA: Association for Computing Machinery, 2021. https://doi.org/10.1145/3442381.3449837

Choi, Hanbyul, Jonghwa Park, and Yoonhyuk Jung. "The role of privacy fatigue in online privacy behavior." *Computers in Human Behavior,* 81 (2018): 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Council of European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.

Council of the European Union. Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2018.

Coventry, Lynne, Debora Jeske, John M. Blythe, James Turland and Pam Briggs. "Personality and social framing in privacy decision-making: A study on cookie acceptance." *Frontiers in Psychology* 7 (2016): 1341. https://doi.org/10.3389/fpsyg.2016.01341

Data Protection Commission, "Guidance note: Cookies and other tracking technologies" 2020. Retrieved from https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance (20.11.2024).

Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. "We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy." In *Proceedings 2019 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society, 2019. https://doi.org/10.14722/ndss.2019.23378

European Data Protection Board. "Statement 03/2021 on the ePrivacy Regulation" Accessed October 21, 2024. https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_en

Fich, Oliver. "The Digital Services Act (DSA) Will Change the Face of Cookie Banners." Cookie Information, September 26, 2022. https://cookieinformation.com/resources/blog/digital-service-act-cookie-banner/.

Habib, Hana, Megan Li, Ellie Young, and Lorrie Cranor. "'Okay, Whatever': An Evaluation of Cookie Consent Interfaces." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–27. CHI '22. New York, NY, USA: Association for Computing Machinery, 2022. https://doi.org/10.1145/3491102.3501985

Judgement of 1 October 2019, Planet49 GmbH, case C-673/17, ECLI: EU: C:2019:801.

Judgment of 4 July 2023, Meta Platforms and Others (General terms of use of a social network), C-252/21, EU: C:2023:537.

Kocyigit, Emre, Arianna Rossi, and Gabriele Lenzini. "Towards Assessing Features of Dark Patterns in Cookie Consent Processes." In: Bieker, F., Meyer, J., Pape, S., Schiering, I., Weich, A. (eds) Privacy and Identity Management. Privacy and Identity 2022. IFIP Advances in Information and Communication Technology, vol 671. Springer, Cham. pp. 165–183. https://doi.org/10.1007/978-3-031-31971-6_13

Lee, P. The impact of cookie 'consent' on targeted adverts. J Database Mark Cust Strategy Manag 18, 205–209 (2011). https://doi.org/10.1057/dbm.2011.20

Leonard, Thomas C., Richard H. Thaler, and Cass R. Sunstein. "Nudge: Improving decisions about health, wealth, and happiness". *Const Polit Econ* 19, 2008. pp. 356–360. https://doi.org/10.1007/s10602-008-9056-2

Mathur, Arunesh, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites." *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 7, 2019): 1–32. https://doi.org/10.1145/3359183

Mejtoft, Thomas, Erik Frängsmyr, Ulrik Söderström, and Ole Norberg. "Deceptive Design: Cookie Consent and Manipulative Patterns." *34th Bled eConference-Digital support from crisis to progressive change, Online, June 27–30, 2021*. University of Maribor Press, 2021, 397–408.

Mejtoft, Thomas, Nike Vejbrink Starbrink, Carla Roos Morales, Ole Norberg, Mattias Andersson, and Ulrik Söderström. "Cookies and Trust." In *Proceedings of the European Conference on Cognitive Ergonomics 2023*, 1–6. ACM, 2023. https://doi.org/10.1145/3605655.3605668

Miniukovich, Aliaksei, Antonella De Angeli, Simone Sulpizio, and Paola Venuti. "Design Guidelines for Web Readability." In *Proceedings of the 2017 Conference on Designing Interactive Systems*, 285–96. DIS '17. New York, NY, USA: Association for Computing Machinery, 2017. https://doi.org/10.1145/3064663.3064711

Naithani, Paarth. "Standardised Cookie Banner: A Solution to the Cookie Consent Problem." *International Review of Law, Computers & Technology*, 1–18. 2024. https://doi.org/10.1080/13600869.2024.2364995

Nouwens, Midas, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. Honolulu HI USA: ACM, 2020. https://doi.org/10.1145/3313831.3376321

Pantelic, Ognjen, Kristina Jovic, and Stefan Krstovic. "Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations." *Sustainability* 14, no. 9 (January 2022): 5015. https://doi.org/10.3390/su14095015

Rossi, A., and Lenzini, G. "Transparency by design in data-informed research: A collection of information design patterns." *Computer Law & Security Review* 37 (2020): 105402

Santos, C., Bielova, N., and Matte, C. Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Technology and Regulation, 2020, 91–135. https://doi.org/10.26116/techreg.2020.009

Santos, C., Rossi, A., Sanchez Chamorro, L., 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 (WPES '21)*. Association for Computing Machinery, New York, NY, USA, 187–194. https://doi.org/10.1145/3463676.3485611

Singh, Ashutosh Kumar, Nisarg Upadhyaya, Arka Seth, Xuehui Hu, Nishanth Sastry, and Mainack Mondal. "What Cookie Consent Notices Do Users Prefer: A Study In The Wild." In *Proceedings of the 2022 European Symposium on Usable Security,* 28–39. ACM, 2022. https://doi.org/10.1145/3549015.3555675

Tankala, Samhita. "Cookie Permissions 101.", Nielsen Norman Group, Accessed September 22, 2024. https://www.nngroup.com/articles/cookie-permissions/

Tomisek, Jan. "Cookies and EU Law: History, Future Regulation and Critique." *Technology and Regulation* 2023 (October 1, 2023): 35–44. https://doi.org/10.26116/techreg.2023.004.

Trevisan, Martino, Stefano Traverso, Eleonora Bassi, and Marco Mellia. "4 Years of EU Cookie Law: Results and Lessons Learned," 2019. https://doi.org/10.2478/popets-2019-0023.

"Web Content Accessibility Guidelines (WCAG) 2.1." Accessed September 19, 2024. https://www.w3.org/TR/WCAG21/

Zachariah, Thejus. "Privacy UX: Best UI/UX Practices for Cookie Consent Banners." *WebToffee* (blog), December 27, 2023. https://www.webtoffee.com/best-ui-ux-practices-for-cookie-banners/