Browser API for managing and recording web consent

Thilak Ramanie Shanmugasundaram
MSc in Computing
Dublin City University
Dublin, Ireland
thilak.shanmugasundaram2@mail.dcu.ie

Apurva Shirbhate
MSc in Computing
Dublin City University
Dublin, Ireland
apurva.shirbhate2@mail.dcu.ie

***Abstract*— Web consent, indicating a user's explicit approval for utilizing online services and aligning with a platform's terms, privacy policies, and data practices, faces challenges with dark patterns and the ephemeral nature of consent. Dark patterns coerce users into accepting terms without proper acknowledgment, and consents accepted are lost when cookies are cleared. Addressing these issues is essential for optimizing consent procedures, promoting transparency, and ensuring users can seamlessly govern preferences across diverse websites, enhancing comprehensive control and data transparency.**

A browser API is one method for controlling and documenting online consent. The openness and control people have over their data can be substantially increased by using a Browser API to manage and record web consent. Adopting a Browser API for web consent management improves user control and data transparency. Consent procedures are streamlined because they make it simple to give or withhold consent and manage preferences across several websites. Businesses gain from this strategy because it guarantees adherence to privacy laws and cultivates user confidence with unambiguous permission procedures. A browser API for permission management fosters user trust, privacy rights, and regulatory compliance all of which contribute to a more open and user-centered digital environment.

Moreover, historical form acceptance rates are significant because they affect online decision-making's transparency, autonomy, and trust. Users can make better selections and grasp the possibility of their form getting accepted when they can access data regarding different forms' acceptance rates. In addition to increasing user confidence in the platform, this transparency gives consumers greater freedom to make their own decisions.

Keywords—GDPR web consent; Dark patterns; Digital Signature; Privacy in web consent

I. INTRODUCTION

The shortcomings of the existing online consent procedures are abundantly evident in an era characterized by strict data security and privacy rules like the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Even with these legal protections for user privacy, research reveals a widespread problem: many websites routinely disregard users' choices about monitoring and consent. In addition to undermining user confidence, this pervasive non-compliance exposes websites to severe financial and legal concerns related to regulatory fines. The current consent management environment, marked by these difficulties, highlights the pressing need for a more dependable and efficient approach. Ultimately, such a system will promote a safer and more responsible digital environment by increasing user trust and autonomy and ensuring website operators can more easily comply with complex privacy rules.

The digital world is changing quickly, and users and regulators are increasingly concerned about privacy. In this regard, implementing a specific browser API for managing and documenting online consent shows promise to improve the online environment and make it more transparent, user-focused, and privacy-aware. An API like this would give consumers more control over their personal information, make consent management easier for website owners, and guarantee compliance with strict privacy laws. This novel technique promises to transform how consent is managed online by enabling the smooth interchange of consent information and promoting interoperability across various websites and platforms. To improve user autonomy, make site owners' compliance more accessible, and foster a transparent and reliable digital environment, this study investigates the possible advantages and ramifications of implementing a

browser API specially made for managing and recording web consent.

Knowing the ins and outs of online consent forms is essential in the digital age, as user consent has emerged as a critical component of data privacy and protection. This study investigates how users' online consent decisions are affected when consent forms' historical acceptance/rejection rates are shown. We explore digital consent's behavioral and psychological dimensions by illuminating how such transparency affects user trust and decision-making autonomy. This method aims to improve our understanding of how users engage with permission mechanisms and evaluate the possibilities of presenting historical data to promote an online environment that is more open, reliable, and user-centered. This study provides essential insights into how permission procedures might be optimized to meet user expectations and privacy laws, ultimately fostering a foundation of informed and self-reliant digital users.

II. METHODOLOGY

The topics for this review were selected by overarching research goals to investigate and address challenges associated with web consent procedures, particularly focusing on issues such as dark patterns, the ephemeral nature of consents, and the potential benefits of introducing a browser API for consent management. Initial research inquiries revolved around understanding the complexities of web consent challenges, examining the impact of dark patterns, assessing the effectiveness of existing consent management practices, and investigating the potential advantages of integrating a browser API. As the review progressed, additional subtopics emerged, including assessing GDPR's influence on web privacy, analyzing consent notices in real-world scenarios, and exploring innovative solutions like Consent-O-Matic and Consent Receipts, incorporating their secure implementation through digital signatures. The methodology involved systematic searches in reputable academic databases using keywords related to web consent, GDPR, dark patterns, and browser API. The inclusion criteria prioritized recent and pertinent research from reputable journals and conferences, thoroughly examining diverse studies that collectively provided insights into the intricacies and opportunities within web consent management.

III. LITERATURE REVIEW

A. *Evaluating GDPR Impact on Web Privacy:*

The study [1] looks into how well the General Data Protection Regulation (GDPR) works for online privacy on EU-based websites serving EU citizens. It finds that although more websites are adopting privacy policies, the application of GDPR, especially in cookie consent notifications, is inconsistent. The study suggests the need for clearer guidelines, especially for issues like user monitoring and cookie consent. It also points out that upcoming regulations, like the ePrivacy Regulation, might help address industry compliance differences and highlight shortcomings in website privacy policies. The study raises concerns about misleading cookie banners, emphasizing that they might not always secure genuine consent and can create a false impression of GDPR compliance. Despite these findings, the study suggests refining regulations and providing clearer guidelines could help overcome privacy challenges.

B. *Navigating GDPRs Impact: Debates, Positive Shifts, and Concerns in the Digital Landscape:*

The investigation [2] delves into debates regarding increased transparency and user awareness using legal analysis and data-driven approaches. While acknowledging positive changes in reduced cookie collection, the paper expresses concern about the complexity of privacy policies and the potential gap between privacy assurances and user understanding. This work contributes significantly to understanding how the GDPR has shaped the digital landscape, bridging legal principles with real-world implications for privacy and data protection on the web. A notable technical weakness lies in the paper's omission of specific GDPR standards, such as explicit consent requirements and data portability.

C. *Studying GDPR Consent Notices in the Field:*

According to study [3], the increase in cookie consent banners has led to greater user fatigue. The analysis delves into the design complexity of consent notices, discusses industry responses and frameworks, and identifies challenges, highlighting

the need for user-friendly solutions. The empirical findings lead to recommendations for optimizing notice design, considering factors like position and language. The study concludes by underscoring the importance of regulations in facilitating a meaningful consent process, offering valuable insights into the evolving landscape of privacy regulations and user interactions with consent notices.

Partial consent was introduced as part of research [4] through a prototype app featuring a "Maybe" button, enabling users to grant temporary permissions. Discovering that 25% of the participants engaged with partial consent, particularly favoring brief consent periods for location data and expressing a preference for the Maybe button for contact access and device memory, the study introduces a notion with potential benefits. Despite limited use, partial consent could enhance user control over personal data without annoying, balancing user convenience and privacy. This study's insights into how users interact with more complex consent alternatives offer valuable lessons that could inform the improvement of suggested API consent management capabilities, making them more adaptable and user-friendly. However, potential issues or gaps in the approach and the feasibility of implementing the "Maybe" button concept would need careful consideration in real-world applications, which would be misused and might cause a few security concerns like data misuse and incomplete revocation, reducing accountability.

D. ***Enhancing Consent Dialog Design through Controlled Experiments:***

The controlled classroom experiment in the research [5] explores user decision-making intricacies, guided by "Choice Proliferation Theory" and "Deception and Social Norms Theory." Investigating the ethical implications of design elements, particularly focusing on the impact of default buttons and introducing the concept of "dark patterns," the study offers valuable causal insights by departing from traditional approaches. Contextualizing historical milestones and privacy regulations, especially the catalytic role of the GDPR, signifies a shift towards a nuanced exploration of psychological factors influencing user decisions. The conclusion advocates for user-friendly interfaces aligned with privacy-aware choices, emphasizing the ongoing necessity for research to refine consent dialogue designs and prioritize user interests. However, the study remained unfinished as the study's conclusions don't align with actual online user behaviours, which can be influenced by a broader array of external factors not fully replicated in the controlled experiment.

E. ***Prioritizing User Interests:***

Focusing on privacy concerns and user skepticism surrounding personal data usage, the research [6] strongly emphasizes prioritizing users' interests during the consent solicitation process, all while ensuring the preservation of their autonomy. It introduces a behavioural approach to the consent elicitation framework to promote moral personal information management and ethical market practices. The paper explores consent's ethical, informational, and marketing implications, including the nuanced consideration that consent may occasionally be given unwillingly yet still deemed valid. A notable contribution is introducing the concept of an "informed attitude" as a crucial component for valid informed consent. The strength lies in providing a comprehensive framework that prioritizes user interests and ethical considerations. The behavioural approach to consent solicitation offers a valuable perspective for fostering transparent and ethical data practices. The notable gap is the need for further exploration into the implications of consent being given unwillingly but still considered valid. While the study acknowledges this nuanced consideration, it could benefit from providing concrete examples or case studies to illustrate how such scenarios might occur in practice. For instance, exploring instances where users feel coerced or pressured into providing consent, yet the consent is legally deemed valid, could offer valuable insights into the complexities of informed consent in digital contexts. By providing specific examples, the research could deepen its analysis of involuntary consent's ethical and legal implications, contributing to a more comprehensive understanding of consent practices in privacy management.

F. Scrutinizing Cookie Banners and Transparency:

In research, [7], a meticulous examination of cookie banner compliance, primarily focusing on IAB Europe's Transparency and Consent Framework (TCF), is conducted. The study employs automated crawls utilizing standard APIs and URL-based techniques to develop automatic methods for TCF banner detection, analyze consent transparency, collaborate with legal scholars, and create tools for violation detection. Legal violations, including pre-stored consent and the absence of opt-out options under GDPR and the ePrivacy Directive, are identified as strengths. Notable findings expose privacy concerns, such as the widespread reuse of identical consent strings. The introduction of Cookie Glasses, a browser extension enabling users to verify consent alignment, proves effective on many TCF websites. However, potential challenges emerge when applying these methods to websites with diverse structures, as the automated tools may face difficulties adapting to unique designs beyond the typical structures encountered in the research. This highlights the need for careful consideration when extending the approach to different contexts with distinct website layouts.

G. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence:

In the exploration presented in study [8], critical issues surrounding digital privacy are addressed by assessing how Consent Management Platforms (CMPs) facilitate users' compliance with GDPR. The study provides a comprehensive overview of the research landscape, contextualizing its examination within the framework of notice-and-consent models and CMPs. By delving into the prevalent "notice and consent" theoretical framework and exploring alternative designs and theories, including the contentious concept of dark patterns, the paper contributes to a nuanced understanding of digital privacy. Utilizing a strong combination of web scraping and field experiments, the research evaluates the designs of popular CMPs and their impact on user behaviour and consent rates.

H. Automated Cookie Consent Detection and the implications of CookieBlocks Solution:

A Notable revelation emerges in [9] with a high non-compliance rate of approximately 94.7% concerning cookie consent on nearly 30,000 analyzed websites. To address this issue, the authors introduce CookieBlock, a browser plugin leveraging machine learning to accurately categorize cookies (84.4% accuracy), comparable to expert judgment. While CookieBlock effectively autonomously blocks 90% of privacy-intrusive cookies without significantly affecting website usability, concerns are raised as it doesn't delve into the reasons users choose to block consent, essentially providing a solution rather than insights into user preferences. The subsequent study [10] validates the technique using a ground-truth dataset of 1,000 websites and tests it on a sample of the top 10,000 websites. Results reveal that while manual techniques efficiently identify consent notices, they may lack comprehensiveness, whereas automated methods like the BERT model are accurate but encounter recall problems due to extraction issues. The research aims to enhance GDPR compliance by improving the identification and assessment of cookie consent notices.

I. Uncovering Unapproved User Tracking Methods in the Post-cookie Era:

The research [11] provides a detailed examination of websites, revealing the extensive use of advanced strategies to circumvent GDPR, underscoring a major strength of the study. It highlights the urgent need for enhanced GDPR enforcement and educational initiatives. However, one potential gap is the lack of detailed analysis of the specific methods employed by websites to circumvent GDPR laws, which could provide deeper insights into the challenges users face in protecting their privacy. Additionally, the study could benefit from exploring potential solutions or strategies to address these sophisticated techniques effectively, thus bridging the gap between regulatory expectations and actual data processing practices.

J. EmPoWeb:

The paper [12] delves into the interaction between browser extensions with high-level permissions and online applications, circumventing the

Same Origin Policy and gaining access to user data, including sensitive information such as bookmarks and login credentials across multiple websites. The study meticulously examines the communication pathways established by extensions in popular browsers, revealing how web apps exploit interfaces to access privileged functions. The paper underscores significant threats to user security and privacy arising from these interactions, emphasizing the urgent need for browser providers to enhance review procedures for identifying and addressing potential security issues associated with extensions. The key factor of the research lies in its comprehensive investigation into the vulnerabilities introduced by browser extensions, shedding light on the potential risks to user data and privacy. Valuable insights can be gleaned regarding the need for robust security measures in the review and approval process for browser extensions.

K. Consent-O-Matic:

Research [13] introduces a browser plugin utilizing adversarial interoperability to control pop-ups based on user preferences. This innovative approach is situated within the broader context of past endeavours to automate user preferences for data processing, acknowledging the limitations of existing standards and privacy-focused browser extensions. The study emphasizes the emergence of Consent Management Platforms (CMPs) in response to regulatory directives like GDPR, highlighting the continuous demand for user-friendly tools in the digital landscape. Additionally, the researchers share insights from their previous endeavour, auto consent, aimed at refining the user experience with consent pop-ups. A notable strength of the research lies in the practical implementation of the browser plugin, not only empowering users to tailor pop-up interactions based on preferences but also offering a dashboard for monitoring consents navigated and the count of clicks saved while using automatic consent filling. Although the research provides valuable contributions to user consent experiences, potential areas for further exploration include getting the website's name, the consent accepted, the list of vendors mentioned by the provider, and displaying the same. This particular gap is one of the main focuses of our research, which will let users understand the type of consent given to a website.

L. Consent Receipts:

The study [14] delves into Consent Receipts, revealing the complex network of online consent management that interacts with technical, commercial, legal, regulatory, and usability factors. The efforts predominantly focus on compliance and emphasis on user-centric solutions. This remains the primary state of the art for this research.

- Exploration of Consent Receipts: The research identifies consent receipts as inspiration drawn from shopping receipts, offering a potential solution to the shortcomings in current consent practices. The study highlights the benefits of receipts for users and service providers, legal compliance, innovation in self-service interactions, and accountability.
- Legal Requirements and Machine-Readable Representations: The research emphasizes the legal foundation of consent, particularly in GDPR. It acknowledges the shortcomings in the current "consent once and forget" model but proposes Consent Receipts to address these issues. However, the debate around the evolving legal landscape, especially regarding international data transfers and changing regulations, still needs to be explored.

M. Web-of-Receipts:

Web-of-Receipts (WoR) framework, a novel solution for valid consent in the digital realm if focused in this research [15]. Focused on secure Personal Data Receipts (PDRs) for consent validation, the framework integrates computer science, law, and public policy concepts, aligning with GDPR requirements. By addressing accountability concerns through a Trusted Third Party (TTP), the research presents a proof-of-concept for WoR, traces consent management's historical development, and advocates for ongoing research. Sound in offering a unique, multidisciplinary framework and outlining future research directions in consent management. However, one potential limitation is the non-implementation of the receipts, leading to the utilization of the proof-of-concept in the proposed solution derived from this research.

N. Ethical and Legal Aspects of Consent Receipts:

Adopting a trans-disciplinary approach, the study [16] integrates insights from HCI, design, privacy, and law, utilizing the "dark patterns" framework to navigate the intricate balance between legal requirements and user experience. Methodologically, it employs interaction criticism and legal analysis, showcasing a shift towards a trans-disciplinary exploration from traditional HCI. The research offers a concise review synthesizing existing research, providing a technical understanding of ethical, legal, and design facets in the context of consent banners and receipts. Strengths lie in the comprehensive, trans-disciplinary perspective, offering insights for future research in ethical design and legal compliance in user interface interactions.

O. Navigating Digital Signatures:

Digital signature technology is a primary challenge when developing web extensions. Study [17] extends this by proposing a method for incorporating advanced digital signature technologies for heightened security. Future work shall involve refining cryptographic protocols, optimizing efficiency, and exploring decentralized identity solutions. While the studies provide valuable information, research fails to explore various kinds of signatures, limiting it to simple electronic signatures(SES). Advanced and Qualified signature leads to an increased level of visibility, authenticity, identity, authentication, and integrity.

P. Examining the Impact of Past Consent on Online Decision-Making:

The study [18] presents a novel strategy for resolving the difficulties of securing informed consent in online research settings. In contrast to conventional, form-based procedures, the project investigates the possibility of improving user involvement and comprehension during the consent process by deploying an AI-powered chatbot named Rumi. By being more understandable and entertaining than standard forms, Rumi, an AI-powered chatbot, provides a novel way to improve online research consent procedures. The prevalent problem of participants skimming or ignoring consent formswhich is troublesome, particularly for sensitive topicsis addressed by this strategy, which prevents participants from making well-informed judgments. Rumi hopes to improve participant comprehension and engagement through conversational AI, democratizing the permission process. This could enhance the caliber of participants' responses and set new moral guidelines for online research procedures.

The paper [19] discusses the challenges big data poses to traditional privacy protections like anonymity and informed consent. It argues that ample data's complex information flows and the ability to make inferences from data undermine these protections, making them less effective in the digital age. The study calls for re-evaluating privacy frameworks to address the unique challenges posed by big data, emphasizing the need for approaches beyond traditional anonymity and consent to protect individual privacy in a data-driven world.

IV. FUTURE WORK:

A. Browser Extension for Consent Receipt Management:

Building upon [14], future work involves developing a Chrome extension focused on storing and managing consent receipts. The technical aspect should include implementing compliance controls within the extension and ensuring user consent actions align with legal frameworks. This involves incorporating mechanisms to display accepted consents and facilitating easy consent revocation. Building upon the "Consent-O-Matic" paper [13], our solution incorporates a machine-readable receipt stored locally. Users can pre-select consent options, and upon providing or rejecting consent, the data is stored in a machine-readable format. Additionally, a clean and user-friendly interface is implemented to display accepted consents.

B. Consent Revocation Mechanism:

The browser API will extend the Web-of-Receipts framework [15] to include a robust consent revocation mechanism within the browser extension. Implement features that enable users to easily identify and revoke consent for specific data transactions. Ensure that the revocation process aligns with GDPR requirements and gives users precise control over their data.

C. *Advancing Web-Consent Management with Extended Digital Signatures:*

The research [17] builds on digitally signing web receipts, proposing future efforts to develop an extensive Browser API to improve web-consent management. This evolution incorporates sophisticated digital signature technologies, elevating the security and reliability of consent agreements. The research will refine cryptographic protocols and algorithms to optimize efficiency and scalability within the proposed API. Another dimension includes exploring decentralized identity solutions, possibly leveraging blockchain or distributed ledger technologies. This advanced approach ensures the seamless integration of digitally signed consent mechanisms, ultimately contributing to an elevated and secure framework for transparent and user-centric web-consent management. Efforts will be made to optimize the efficiency and scalability of signature generation and verification processes within the API, considering factors like computational overhead and latency.

The paper [17] examines the use of Zero-Knowledge Proofs and Homomorphic Encryption to enable data tracking without breaching user privacy. Additionally, integrating decentralized identity protocols should enhance user control. Research efforts will focus on seamless API integration into popular browsers, promoting widespread adoption and empowering users with unparalleled transparency and consent management capabilities.

D. *Empowering Users through Educational Component:*

As a pivotal aspect of future enhancements, we envision the integration of an educational component into the Chrome extension. This supplementary feature will serve as an add-on, giving users valuable insights into diverse consent designs, potential dark patterns, and their rights under the GDPR. The overarching objective is to empower users by clearly explaining consent-related practices on various websites. This initiative aligns with the paper's [20] overarching emphasis on advancing user understanding and decision-making within the notice-and-consent model. This supplementary component is an additional task achievable upon accomplishing the primary research objective.

E. *Analyzing Consent Histories: User Autonomy and Trust:*

Our study aims to explore how displaying historical acceptance/rejection rates of consent forms influences user decisions in online consent scenarios, focusing on the roles of transparency and trust in enhancing decision-making autonomy. It seeks to understand if such disclosure impacts users' perceptions of platform integrity and the reliability of the consent process, potentially leading to more informed choices. By examining the effect of past consent decisions on current user behaviour, the research investigates whether increased transparency can bolster user trust and autonomy, aiming to create a more user-centric online environment.

As discussed in the paper [18], the chatbot-enhanced consent procedure presents a fresh angle on user involvement and decision-making in online consent scenarios. The findings on enhanced user comprehension and satisfaction through interactive, conversational interfaces can be extrapolated to suggest that transparency and user autonomy are critical in online consent, even though they do not specifically address the effect of presenting historical acceptance/rejection rates. By increasing openness and trust, this strategy may suggest that providing past rates in an exciting and user-friendly waypossibly via chatbots or other such technologiesmay benefit users' judgments regarding consent.

Through highlighting the intricacies of data usage and user autonomy in online contexts, the paper [19] focuses on the issues big data presents to privacy protections and how they connect to the presentation of historical consent rates. By giving users more insight into consent procedures, transparency in historical rates could improve user trust and autonomy in making decisions. This transparency suggests a shift toward more informed and user-centric permission methods in the digital age. This aligns with the paper's proposal for changing privacy rules to handle significant data concerns.

V. Conclusion

The proposed Browser API and Chrome extension aim to revolutionize web consent management. The extension focuses on efficient con-

sent receipt storage and management, incorporating compliance controls and a user-friendly interface. A robust consent revocation mechanism aligned with GDPR standards enhances user control. The advancement of web-consent management includes extended digital signatures, refining cryptographic protocols, and exploring decentralized identity solutions. This ensures a secure and reliable framework, with efforts to optimize efficiency and scalability. Moreover, an educational component in the Chrome extension empowers users by providing insights into consent designs, highlighting potential dark patterns, and educating users on GDPR rights. The approach emphasizes user trust, privacy rights, and regulatory compliance in a user-centered digital environment.

Incorporating historical consent rates on online platforms can enhance user decision-making, foster autonomy, and increase trust. This method helps users assess the likelihood of success for their actions by offering vital information about platform operations. By fostering an informed user base, such transparency enhances the digital experience. However, the effects of past rates are complex and vary depending on contexts for consent, interface design, and personal privacy concerns. These elements affect how trustworthy users believe a platform to be and could result in different reactions depending on what their peers do.

REFERENCES

[1] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz, "We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy," *arXiv preprint arXiv:1808.05096*, 2018.

[2] D. Anderson and R. von Seck, "The gdpr and its impact on the web," *Network*, vol. 1, 2020.

[3] C. Utz, M. Degeling, S. Fahl, F. Schaub, 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*, pp. 973–990, 2019.

[4] S. Bock, A. F. Chowdhury, and N. Momen, "Partial consent: a study on user preference for informed consent," in *HCI International 2021-Late Breaking Papers: Design and User Experience: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings 23*, pp. 198–216, Springer, 2021.

[5] S. Korff and R. Böhme, "Too much choice: End-User privacy decisions in the context of choice proliferation," (Menlo Park, CA), pp. 69–87, USENIX Association, 2014.

[6] G. Burkhardt, F. Boy, D. Doneddu, and N. Hajli, "Privacy behaviour: A model for online informed consent," *Journal of business ethics*, vol. 186, no. 1, pp. 237–255, 2023.

[7] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europes transparency and consent framework," in *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 791–809, IEEE, 2020.

[8] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. 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*, pp. 1–13, 2020.

[9] D. Bollinger, K. Kubicek, C. Cotrini, and D. Basin, "Automating cookie consent and {GDPR} violation detection," in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 2893–2910, 2022.

[10] R. Gundelach and D. Herrmann, "Cookiescanner: An automated tool for detecting and evaluating gdpr consent notices on websites," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, pp. 1–8, 2023.

[11] E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, and E. P. Markatos, "User tracking in the post-cookie era: How websites bypass gdpr consent to track users," in *Proceedings of the web conference 2021*, pp. 2130–2141, 2021.

[12] D. F. Somé, "Empoweb: empowering web applications with browser extensions," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 227–245, IEEE, 2019.

[13] M. Nouwens, R. Bagge, J. B. Kristensen, and C. N. Klokmose, "Consent-o-matic: Automatically answering consent pop-ups using adversarial interoperability," in *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pp. 1–7, 2022.

[14] V. Jesus and H. J. Pandit, "Consent receipts for a usable and auditable web of personal data," *IEEE Access*, vol. 10, pp. 28545–28563, 2022.

[15] V. Jesus, "Towards an accountable web of personal information: The web-of-receipts," *IEEE Access*, vol. 8, pp. 25383–25394, 2020.

[16] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark patterns and the legal requirements of consent banners: An interaction criticism perspective," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–18, 2021.

[17] G. R. Haron, N. I. Daud, and M. S. Mohamad, "Narrative of digital signature technology and moving forward," *Int J Intell Comput Res (IJICR)*, vol. 10, no. 3, 2019.

[18] Z. Xiao, T. W. Li, K. Karahalios, and H. Sundaram, "Inform the uninformed: Improving online informed consent reading with an ai-powered chatbot," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1–17, 2023.

[19] S. Barocas and H. Nissenbaum, "Big datas end run around anonymity and consent," *Privacy, big data, and the public good: Frameworks for engagement*, vol. 1, pp. 44–75, 2014.

[20] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems: A user study of consent dialogs after gdpr," *arXiv preprint arXiv:1908.10048*, 2019.