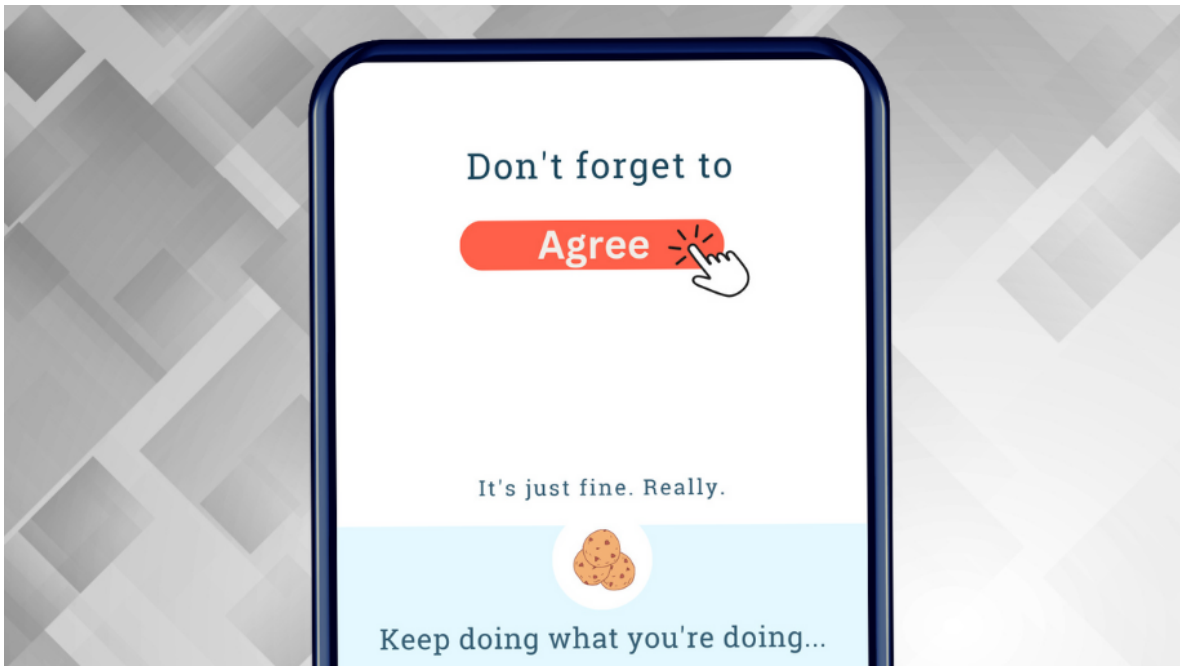
From Policy to Pixels:

Strategic UX Design and User Support for GDPR Implementation

superbloom



Key words
GDPR, consent, cookie banners, design practice

Authors
Susan Kennedy, Ame Elliott

Date
10/17/2023

Table of Contents

Abstract

To situate General Data Protection Regulation (GDPR) policy implementation in current user experience design (UX) practices, we report findings from qualitative interviews with five designers and front-end developers experienced in creating cookie banners. In exploring how multi-disciplinary product teams reach design decisions, we found that discussion about cookie banner implementation centers on compliance legalese rather than interactive, usable visual elements that enable active choice. We propose a preliminary framework of personas (archetypal profiles) for capturing a range of attitudes towards GDPR cookie consent compliance and graphical implementation. Using these personas to evaluate existing tools for cookie management, we identified a gap in the tooling and support ecosystem that can meet the needs of people without specialized legal knowledge, technical skills, or large budgets, but who are eager to tailor a cookie banner experience to meaningful, user-centered consent. Equipping people without specialized domain knowledge or personal passion for privacy to participate in discussion about GDPR cookie consent implementation is essential for shifting the status quo and making informed consent a reality.

Part 1. Introduction

GDPR in context

The intention, in part, of the European Union's General Data Protection Regulation (GDPR) and similar laws is to protect users' privacy and autonomy by ensuring they have the right to choose whether third parties collect their personal data and how their data is used. In order to make an informed choice, the user must be presented with clear information and must be able to easily navigate the interface to make an accurate selection. The typical graphical implementation of GDPR consent requirements is via cookie consent banners; the pop-up boxes users see upon opening a web page which are ostensibly meant to inform the user of their rights to opt-in to personal data collection. However; as shown by many studies, there is misalignment of data privacy policy intentions with real world design implementation. herefore, the average user's experience is not supported by a fully informed and active choice. Although it has been shown that most users would not opt-in to data collection under GDPR, in practice they quickly click through the cookie banners, unknowingly consent to data collection without fully understanding what they are consenting to, and view the process as a disruption to their flow. This current reality neither protects nor informs the user, and maintains the status quo of mostly unrestricted user data collection for business profit and other motives. Industry is incentivized then, to maintain the current design of most cookie banners, as more users consent to data collection than would if they were adequately informed and presented with a clear consent process.

There is an opportunity to better realize data privacy policy intentions by establishing requirements for informed, innovative, quality UX design that implements these policies by centering the end user's experience and needs. In addition to the need for improved user interfaces designed around the habits and psychology of users, the language used in cookie banners needs to be fully understood by a wide range of users. Front-end implementers (designers and developers) and legal teams need to work more collaboratively with each other in

creating cookie banners that are easy for the user to navigate, read, and comprehend.

Under rights-based laws, users have the right to make informed decisions about whether or not companies can collect their personal data. In the case of the GDPR and other such laws, user decisions are active. Users must “opt-in“ to data collection for a company to collect data, and therefore, when first entering a website, a user’s right to choose must be explicitly clear. Under the California Consumer Privacy Act (CCPA) and other United States based state laws, the requirement is for users to have the choice to "opt-out" of data collection, an action which is on the user to pursue. In those cases, it is not required for a user to be greeted with a consent banner upon entering a site, although some companies bound by these laws choose to use them.

Because the GDPR and other laws do not yet include extensive design and language requirements,[1] businesses implementing consent policies must shift their focus from mere compliance with the law to an ethos and practice of proactive protection of user choice through meaningful, informed user consent processes. This can be ensured through usable, clear, and seamless consent notices. Policies can and should be adapted to require specific design and clear language requirements. However data protection laws are worded, there needs to be more dialogue across all stakeholders involved in the design, and implementation of consent notices. Designers, developers, managers, policymakers, and lawyers need to collaborate in understanding the importance of design and language decisions for effective implementation of consent-based data privacy policies.

To better understand the current dynamics among these different actors, we interviewed five EU-based designers, developers, and product professionals who have created cookie banners.

[1] *Effective as of March 29, 2023 California established some of the most expansive language and design requirements seen in data privacy law regulation. It included principles around design and language with limited examples as part of its updated regulations for the amended California Consumer Privacy Act of 2018. Although these requirements do apply to consent banners, cookie banners or similar landing page consent notices are not required as part of CCPA.*

As designers and researchers at Superbloom, it is our mission to change who technology serves through the power of trustworthy design. Our goal was to situate GDPR policy implementation within current professional UX design practices and experiences. We wanted to understand how multi-disciplinary product teams reach design decisions, how familiar they are with the laws, what challenges they face in implementation and compliance, and their overall goals and perspectives relating to user data protection. With the introduction and enactment of other data privacy laws around the world such as the proposed federal Online Privacy Act of 2023 in the United States and the passing of the Digital Services Act (DSA) in the EU, there is an opportunity to build on these learnings as global policies evolve, regulations are defined, and enforcement begins.

We synthesized the qualitative interview findings into a preliminary persona framework and used participant-led discovery to evaluate how well a range of cookie management tools performed. We expanded on the tools mentioned by participants to understand how these might meet the needs of the various personas for implementing cookie banners. Through this process, we identified a gap in available cookie management tools and resources, and found many fail to meet the need for multi-stakeholder collaboration. We conclude by discussing potential directions for businesses and designers to adequately equip users with the information and experience needed to exercise their rights under data protection policies.

Background

Cookie banners are the ubiquitous interstitial dialogue boxes found on every web page in the EU – and much else of the world – that allow users to consent to or reject personal data collection in accordance with data protection laws. Despite this purpose, cookie banners fail to inform or protect users at the level they should. Several studies have shown that most EU web users quickly click through website cookie banners, view banners as a disruption to their goals in visiting a site, leading them to often believe they have opted out of consent when they have in fact unknowingly opted in.[2] There are many reasons for this, ranging from

[2] doi: 10.1145/3313831.3376321; doi: 10.1145/3319535.3354212

intentional (manipulative) and unintentional design choices; to user comprehension and impatience. However; it is a fundamental tenet of UX design that products are designed to be easy to use, regardless of the users' knowledge or level of patience. Instead, design must meet users where they are, and not expect users to jump through hoops to access information or services.

On top of frequent usability challenges found in cookie banners, companies sometimes leverage "deceptive design" (also known as "dark patterns") to bypass legal requirements set by data protection authorities. Deceptive design practices in cookie banners deceive the user or manipulate them into consenting to data collection because of underhanded design choices made in the implementation process, such as default checking the "opt-in" consent choice, displaying the "opt-in" more prominently than the "opt-out," or making the user navigate a maze of pages to opt-out.[3] A user study from 2020 found that "dark patterns and implied consent are ubiquitous; only 11.8% meet the minimal requirements" that the researchers set based on articles of the GDPR.[4]

These deceptive practices are being noticed more by policy makers. Improvements include the 2023 amendments to the CCPA outlining design and language requirements for consumer consent notices, the prohibition of dark patterns in the DSA, and GDPR updates that ban certain deceptive practices, such as "cookie walls" (the disruptive full-page cookie dialogues that makes it impossible to access a site without consenting)[5]. The increased recognition of design elements impacting user choice and agency is a critical step forward, but there is room for policymakers to outline further UX design and user accessibility requirements as core tenets of privacy laws such as the GDPR and the CCPA.

---

[3] doi: 10.1145/3313831.3376321; https://dl.acm.org/doi/abs/10.1145/3411764.3445779; doi: 10.1145/3400899.3400901; https://www.stiftung-nv.de/en/publication/dark-patterns-regulating-digital-design; https://www.gmfus.org/news/designing-against-dark-patterns; https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/; doi: 10.1093/jla/laaa006.

[4] doi: 10.1145/3313831.3376321

[5] https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065/; https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-art-60-gdpr-guidelines-dark-patterns-social-media-platform_en.

Researcher, Caroline Sinders, proposed a set of design principles that could be added to the GDPR and similar laws to both promote user agency and restrict deceptive design practices by companies.[6] These principles aim to promote user comprehension and experience of cookie banners, which would ultimately increase rates of informed consent.

In "Designing Against Dark Patterns," Sinders proposes the following principles:

- Platform policies and settings should take platform "main real estate" as opposed to being hidden, and be easy to find.
- Platforms should use plain language, and elements that introduce friction allow users to understand and act on information.
- There should be increased cross-platform standardization to aid user agency in completing tasks and editing settings.
- Policymakers should require consistent and legible user interface design, which would display consent-based choices equally in a visual hierarchy and would ensure consistent color and design choice in interstitials to avoid confusion. Such a requirement avoids undue influence on a user through suggesting a company's perceived preference for a specific choice."[7]

In addition to considerations about the design of cookie banners, there is growing evidence to support that the language used in the banner is just as essential for user comprehension and trustworthy consent. Researchers have found that the language of popular sites' cookie banners often violate several GDPR legal requirements.[8] These include the requirement for sites to state the "explicit and specific purpose" of the data they're requesting to collect; and that language must be "intelligible," "freely given," and "informed consent written clearly and plainly" – i.e., that it is free of jargon and easy to follow and understand.[9] The same study found that 89% of sites researched violated the law through their use of language on their cookie banners.[10] Although the law clearly states certain language requirements, the lack of specificity makes it so

[6] https://www.gmfus.org/news/designing-against-dark-patterns
[7] https://www.gmfus.org/news/designing-against-dark-patterns
[8] https://dl.acm.org/doi/abs/10.1145/3411764.3445779
[9] https://gdpr-info.eu/
[10] https://dl.acm.org/doi/abs/10.1145/3463676.3485611

that implementations are inconsistent and regularly skirt requirements through vague, jargon-filled, confusing, and/or redundant language.

The updated CCPA regulation provides more specificity, stating that businesses using consent notices must "design and implement" various UX and clear language best practices. Among other requirements, it states that businesses must ensure consent text is "easy to understand", that there is "symmetry in choice", that the process does not include "unnecessary burden or friction" for the user, and prohibits the use of dark patterns.[11] This level of detail is a big step forward regarding language and design guidance, but it is too soon to understand how these regulations may be effectively enforced, and may be complicated or overridden by some of the more controversial aspects of the law.[12]

Nonetheless, the studies named above demonstrate a need for better understanding of both the design and legal processes involved in creating website cookie banners and other consent policy design implementations. As policy shifts and technology evolves, there will be a continued need for collaboration among stakeholders designing, implementing, and enforcing policies to best understand the nuances of user experience design and how it is a critical component of an effective data privacy law. In our research specifically, we sought to explore how front-end design implementers and legal teams interact, and based on the research, define the resources they need to build effective, consentful, user-friendly cookie banners.

Methodology

We conducted five semi-structured qualitative interviews with implementers (UX/UI designers and front-end developers) tasked with upholding GDPR data-consent requirements through cookie banners. These anonymous interviews were held under rigorous privacy-preserving conditions, allowing for transparent perspectives on employers, colleagues, policies, and the industry. Interviewees were offered a stipend of 100 Euros for 60 minutes of their time.

[11] https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf
[12] https://epic.org/californias-proposition-24/

Interviewees were recruited through multiple design and product professional channels. Despite broad outreach, we received surprisingly few responses, however; the individuals who did self-select were strongly committed to privacy practices and knowledgeable about policies such as GDPR. Should we expand this study, we will aim to specifically recruit designers and developers with less knowledge about privacy laws and less explicit passion for user data protection. This would help us understand the perspectives of a more representative group that feels ambivalent about the policies or sees it chiefly as a work assignment and not necessarily a personal moral obligation to protect data. It would be equally useful to hold a round of interviews with compliance lawyers in order to hear their perspectives on, and challenges around, design implementation when it comes to legal concerns. A further hypothesis that could be tested as well, is whether or not designers and/or front-end developers have any anxiety about what their personal liability may or may not be with respect to implementing the law via design. Overall, there is a strong need to examine the effectiveness and implementation challenges of consent notices under non-EU and North American policies, such as the Brazilian Data Protection Law (LGPD) and the Thailand Personal Data Protection Act (PDPA).

We asked questions about the interviewees' general knowledge around GDPR, their roles, the roles of their team, their experience with implementation of the policy, the resources available to them, the dynamics within their team, and the challenges they faced. The full set of interview questions is available in Appendix A.

Building on our interview findings, we investigated the products and services that participants mentioned as tools and resources they use for supporting policy design implementation. These ranged from premium paid subscriptions for data handling services to open source code available for download on GitHub to WordPress plugins. We conducted preliminary competitive benchmarking using cognitive walkthroughs of product websites, paying special attention to how websites describe their products' value to people tasked with implementing cookie banners.

Part 2. Interview Findings

_____

Implementing GDPR in the real world

We expected to hear stories of designers and implementers pressured into designing banners that solicit as many opt-ins to data collection as possible, yet surprisingly those stories rarely arose in our conversations. Although someone shared that during a stressful first week in a new job as a junior front-end developer, they were tasked with implementing cookie banners across the whole company. Direct pressure to find ways to encourage data collection (beyond basic compliance) did not feature as prominently as expected in our interviews. Our findings below highlight the role that domain experts comfortable with legal text play in shaping the ecosystem.

Privacy-conscious participants

Although we expected designers would be ambivalent about privacy (or at least see it as outside of their remit), our research participants were active advocates for data privacy and privacy-conscious in their work. One explanation for this unexpected finding is sampling bias. We intentionally sought out people in mainstream industry design communities, such as alumni networks of design consultancies, a Slack group for corporate design leaders, LinkedIn, and Twitter. We did not include criteria in our recruiting, such as attitude towards GDPR. We wanted a snapshot of current mainstream industry practices and intentionally avoided outreach to communities with a known pro-privacy stance, such as the Human Rights Centered Design community, or the Open Technology Fund discussion group. Despite this outreach strategy, all five participants self-selected to participate on the basis of their strong interest in GDPR and the design implementations of policy. Attempts to encourage participants without particular privacy-domain knowledge, particularly Americans who have not had exposure to implementing consent designs, were rebuffed, with responses such as “I don’t know enough about the topic to be helpful”.

Compliance does not mean usable

Although each team behind a website and its data collection protocols is different, compliance with data protection laws to ensure meaningful user consent was more preferred than usability. Compliance is of course critical for business sustainability, as are the preservation of companies' websites and web-based products.But we should ask why the current model is to defer to lawyers and compliance in its most literal sense, and not refer to UX professionals' expertise in promoting user engagement and comprehension through thoughtful design. The usability and functionality of cookie banners are just as important as quality and compliant language,and teams with multi-faceted expertise should work collaboratively to create a balance of all these features. After all, is it compliant if users don't understand what they are consenting to? Under some laws the answer may be ambiguous or not addressed, and in others where user comprehension is required, there may not be sufficient examples and challenges to enforce.

To better understand a user's understanding of their rights and choices using cookie banners, one designer we spoke with conducted studies that further verified this phenomenon:

> *We did two rounds of studies. A survey and observations and recording interactions of people with two different cookie banners. We wanted to understand what people understand and what they declared to do when confronted with a cookie banner. People were saying they either refuse cookies or set preferences. But [there is] 80-90% consent for cookies.*
> *– Designer, Government Agency*

The dialogue between implementers and lawyers need to be proactive, and question what is necessary versus what is a recommendation. As one interviewee said:

> *One of our lawyers would change wording, add five paragraphs – and we would say, why would we do that? We would ask if this is a requirement or recommendation. We would say: thank you for your opinion. What is the bare minimum to do this?*
> *– Senior UX Designer, Industry*

Another interviewee had the idea of starting a practice for front-end implementers, in which they show examples of usable language in cookie banners with legal teams. They said:

> *People want to build a good product, but often these things are complicated because of legal stuff. Lawyers write the text. Having examples to send to the legal department can be helpful. Lawyers don't know how to [write for on-screen dialogue boxes] well. Good examples would help a lot.*
> *– Founder, Mobile App Development Studio*

Cultural friction with lawyers

Each one of the front-end implementers we interviewed talked about challenging design dynamics when working with lawyers and legal text to create usable cookie banners. Ultimately, lawyers, designers, and developers speak and complete work tasks using different professional languages – respectively legal text, visual design, and code. This creates communication tensions among the team. Knowing that the typical cookie banner is not easily understood by users or effective in their ostensible intent, we sought to understand if communication and translation challenges impacted poor design.

In our five hours of conversation, we heard only one (expected) story of a client pressing business metrics onto front-end implementers to pressure them to trick users into consenting: one interviewee talked about the challenges they faced working with a European sports company, experiencing pressure to design in a

way that promotes user data collection. This privacy-conscious interviewee chose to cut ties with the business over this misalignment in values. Not everyone has the flexibility to give up work over principles, and in some cases less privacy-conscious employees might respond to such requests as business-as-usual.

“

There was a hierarchy where the advertisers want something, the client wants something, the user wants something. In the end, you can’t control everything. That’s the hierarchy – where the money comes from is where the decisions come from.
– Founder, Mobile App Development Studio

In our interviews, we unpacked some of the dynamics behind the decision-making hierarchy, and found that the tension around complicated, jargon-filled text plays a central role in the conversation around cookie banner design. That is, when discussing GDPR implementation, the pixels most under discussion are textual rather than graphical. Writing interface copy – the text appearing in buttons and dialogue boxes – is a subspecialty of user experience design. In most professional user experience design contexts, interactive visual design elements dominate discussion (e.g. if the default state of sliders appear grayed out or not or if the user's eye is drawn to the important buttons.) However; in the case of cookie banner implementation, the primary questions and challenges designers and front-end developers had were around the application (or not) of compliance legalese into the cookie banner.

Lawyers favor dense text

“

Working on text is always complicated when you work with lawyers.

– Designer, Government Agency

In our interviews, we heard again and again that complicated, confusing legal text is a major design barrier for creating user-friendly cookie banners. Although each interviewee had different levels of exposure and interaction with lawyers – some in-house, and some consulted – each faced a similar challenge of back-and-forth discussions about the use of language in cookie banners. This back-and-forth plays out similarly among each; the lawyers would recommend a wall of complicated legal text; and the implementers would explain that no one reads walls of text, that with that constraint it would be impossible to design an effective, user-friendly consent model. Ultimately, designers agree that complicated, lengthy text creates undue friction and turns users away. Often, lawyers had the last word, but in some cases, designers were able to push back.

Existing research backs up the experience of the front-end implementers. The language used in cookie banners is confusing to users; many misunderstand the meaning, don't read it at all, or believe they've opted-out when in fact they've opted in.[13] Ironically, at the same time, cookie banners rarely use language in a way that's actually compliant with the law.[14]

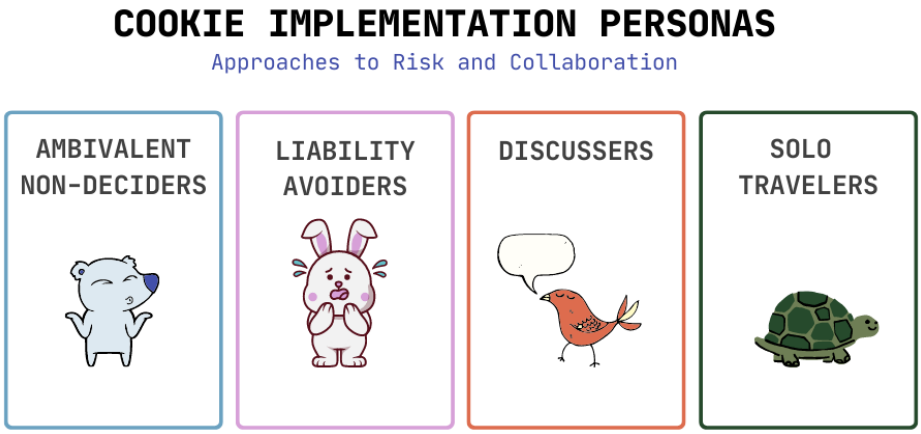
Why would lawyers in these cases work so hard to advocate for large blocks of text, if in fact users don't actively consent, and the language doesn't fundamentally respect the GDPR requirements for "explicit, specific purpose", "intelligible", "freely given", and "informed" consent to be written clearly and plainly?[15] This is an open question, but at least speaks to the need for better communication and collaboration between actors to ensure that all goals are being met. The following section is an initial attempt to codify some of what we heard about how non-designer stakeholders shape cookie banner discussions and design decisions.

[13] doi: 10.1145/3319535.3354212; doi: 10.1145/3313831.3376321
[14] https://dl.acm.org/doi/abs/10.1145/3463676.3485611
[15] doi: 10.1145/3319535.3354212; doi: 10.1145/3313831.3376321; https://gdpr-info.eu/

Part 3. Personas

Tools for building shared understanding

Personas are a profiling tool used for clarifying and documenting user needs by creating exploratory archetypes grounded in user research. Using the data from our interviews, we leveraged this user research tool and created four personas as a preliminary framework for classifying approaches to cookie management.



Cookie banner implementation personas

We wanted to understand how multi-disciplinary product teams reach design decisions, their familiarity with the laws, challenges they face in implementation, and their overall goals and perspectives relating to user data protection. In summarizing the types of approaches, we created four profiles with divergent approaches: Ambivalent Non-Deciders, Liability Avoiders, Discussers, and Solo Travelers.

Ambivalent non-deciders

❝

My first task when I moved to the Community team was when someone complained about the lack of cookie consent, I had to add it. No one cared about it, I was a junior developer, and I was tasked to do this across the whole company.
– Front-End Developer

Ambivalent managers and teams don't consider compliance an organizational priority and take a laissez-faire attitude to implementation. The lack of certainty in enforcement is seen as permission to have no solution and take a wait-and-see approach. Compliance is a low priority and changing the status quo requires a specific complaint or known threat. If compliance is a low priority, then thoughtful user-experience design working toward user comprehension is an even lower priority. Since the work is not prioritized, the implementers are likely to lack resources.

Liability avoiders

❝

I understand that people [managers] don't read regulations with a precise eye. People are scared, thinking they need to hire help.
– Freelance/Volunteer Designer and Front-End Developer

In contrast to Ambivalent Non-Deciders, Liability Avoiders consider enforcement ambiguity as a dangerous liability that threatens their organization. This group is enthusiastic about legal expertise and their organizations lean heavily on legal advising. The lawyers' directions are very challenging for front-end developers to implement because the lawyers request extensive legalese in the interface, and they consider any deviation from the strict legal text a threat. Liability Avoiders

are attracted to the value propositions of cookie management services such as One Trust, which above all promote compliance over user comprehension, and they are open to paying money so as to minimize risk.

Discussers

“

I look at the legal team as advisors. They should not be dictating what products we can and cannot build. They need to provide advice. We've had a couple situations where it's a full page of large text. We shared our competitor's page – they provide a link to the text. ... Can we still meet the letter of the law without destroying usability of the product?
– Senior UX Designer, Industry

Discussers actively engage in dialogue with multiple stakeholders about cookie management, and present an opportunity for intentionally shaping practices. Despite good intentions, the collaborative process between different stakeholders can be strained because of the lack of shared vocabulary between lawyers and implementers. A particularly significant communication challenge is whether or not to center legalese, which is a barrier for even policy-literate designers to overcome. By discussing options and providing examples, case studies, and best practices, designers and front-end developers can shape compliance conversations around user needs.

Solo travelers

“

The artists I work with see the legal language and say it's too complicated.
– Freelance/Volunteer Designer and Front-End Developer

Four of our five interviewees discussed implementing cookies in a commercial context, but we spoke with one individual who worked as a freelancer and volunteer building websites for artists and charities. These clients had limited

resources, and mostly needed to re-use and adapt cookie banners they found elsewhere online. The interviewee said that these clients were very unsure and nervous about compliance, and rarely understood the policies.

They also warned of clients being targeted by scams, where they are threatened and told that their websites will be reported unless they pay a fee to “fix“ their cookie banners and improve overall data compliance. Many times, according to the interviewee, individuals are pressured to pay money they don’t have for reused cookie banners that are not relevant to their situation, contain inaccurate information, and do not comply with regulations. Avoiding such risks in a responsible way ultimately requires resources, expertise, and time.

One alternative is to use free online templates, but end-users without the support of larger organizations and legal teams do not necessarily understand what they're using, know whether the templates are up-to-date and/or accurate, or which one might apply to their particular situation. The same interviewee shared an anecdote:

> *“*
>
> *A lot of people use some templates and don’t try to understand, they just change the date and the company name on something that is already applied to their website. I saw some info and services which are not used on that particular website - but it was copied, and they didn’t have the basic knowledge. They didn’t even realize they don’t have cookies like that.*
> *– Freelance/Volunteer Designer and Front-End Developer*

In summary, a one-size-fits-all approach is unlikely to be successful at covering the goals, concerns, risks, and needs in different business contexts.

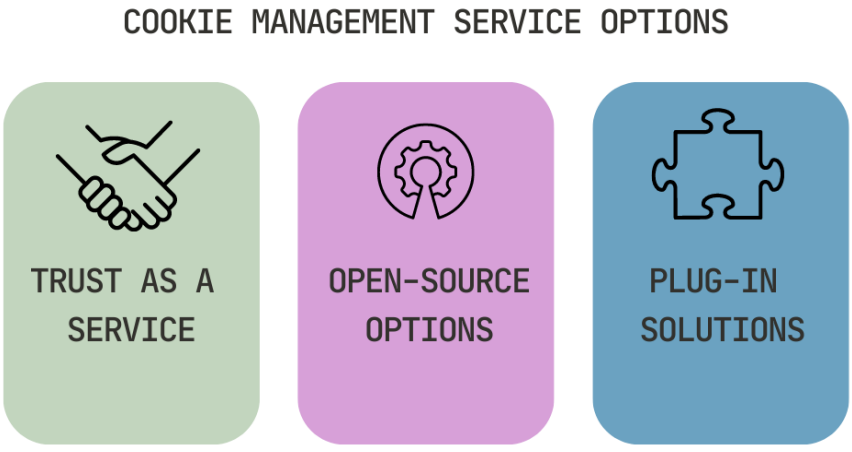
Part 4. Discussion

Implications for cookie management

In our interviews, our participants spoke of cookie management tools they have used or heard of. We analyzed these tools to understand their advertised purpose, their use, and relevance in given context. Our exploration was informed by cognitive walkthroughs, putting ourselves in the mindset of one of our personas, and evaluating the interfaces of cookie management options through their eyes. For example, a beginning of a walkthrough scenario might look like:

“You are a Solo Traveler who needs to make a WordPress website GDPR compliant. With limited time and resources, we begin by entering search terms into Google and note the steps and setbacks on the path to successful implementation of cookie banners.”

After engaging in these walkthroughs, we hypothesize that there are three levels of cookie management tools that span the needs of our personas.



Cookie management service options

Trust as a service

Popular consent management providers (CMPs) like One Trust, QuantCast, and Cookiebot are paid services that provide customizable templates for data protection policy compliance in multiple jurisdictions.[16] The cookie banner designs for these services have limited design customization features, such as the ability to change color and font. The language used in banners is central to their main value proposition: delivering legally compliant products to their clients. However; researchers have found that "illegal practices prevail" in these products "with vendors of CMPs turning a blind eye to — or worse, incentivising — clearly illegal configurations of their systems."[17] Additionally, we heard from interviewees that although it was easier to have a service to use than start from scratch, CMPs are typically more complicated to implement than it might at first seem. These services target Liability Avoiders anxious about compliance, who have money to spend on mitigating their risk with legalese over effective user-design. These companies' value propositions advertise a sense of safety or relief for Liability Avoiders. Walking through the One Trust website, there are many educational resources targeting a non-technical audience, which promote the maximization of user opt-ins to data collection.

> *"*
>
> *OneTrust cookie consent enables companies to uncover hidden cookies and trackers on websites, configure branded banners using unique consent approaches based on location, and measure and optimize consent rates for maximum opt-ins.*
> *– OneTrust.com Cookie Consent Demo*[18]

The messaging and tone of premium services emphasize that trust management is complex, and that the provider has already made the hard compliant decisions, and all businesses have to do is implement their out-of-the-box solutions. The

[16] https://www.onetrust.com/; https://www.quantcast.com/products/choice-consent-management-platform/; https://www.cookiebot.com/en/
[17] doi: 10.1145/3313831.3376321
[18] https://www.onetrust.com/resources/cookie-consent-demo/

target audiences are Ambivalent Non-Deciders with deep pockets, and Liability Avoiders.

Open-source options

At the other extreme, for those looking at an external service or tool to assist with implementing compliant cookie banners, one option is a do-it-yourself approach targeting knowledgeable front-end developers. Osano and Tarte au Citron offer cookie management open source code. In contrast to the polished marketing messages of One Trust, these projects foreground data-privacy values and use GitHub pages to distribute the code, although there are minimal examples and little context.[19] These tools target people strongly interested in privacy-preservation with enough technical skills not to be intimidated by code, and implement more customization themselves. Industry-based Ambivalent Non-Deciders, Liability Avoiders, and Discussers are not likely to know about these and other open source, privacy-focused tools unless they already work with a lot of open source software or are in privacy advocacy circles. And, they would have to commit time and money for a developer to implement these tools. From a cost-saving perspective, a skilled Solo Traveler might be most incentivized to use these tools, and, if they're particularly privacy-conscious, from a values-alignment perspective.

Plug-in solutions

Our interviewees mentioned using WordPress plugins to manage cookies, and searching for "cookies" in WordPress plugins yields 51 pages of results for cookie management options. Solo Travelers who do not identify as front-end developers but maintain and design WordPress sites may find these options attractive. Similarly, Ambivalent Non-Deciders in charge of WordPress sites could use this resource to build on top of existing uses. However plugins, templates, and reusable code are not easily discovered or implementable by non-technical people. As an Ambivalent Non-Decider, walking through steps to successfully implement cookie management, it's easy to conclude that technical skills as well as time are requirements for compliance.

[19] https://github.com/osano; https://tarteaucitron.io/en/

Little middle ground

In our research, there were few success cases of designers and other business stakeholders (especially lawyers) collaboratively discussing options for compliant yet user-friendly cookie banners. These cases fit the mold of the “Discusser“ persona. But, as a curious Discusser approaching the path to successful cookie banner implementation, there is no obvious choice of a CMP or open source code that allows substantive and nuanced design and compliance customization, nor any that might facilitate and respond to discussion between actors. Discussers uncomfortable with dense legalese have a difficult time joining a conversation about cookie banner implementation. This presents a major opportunity to engage more stakeholders from a broader range of backgrounds in conversation, and design of CMP and open source tools that facilitate better collaboration and customization of user-experience and language.

Part 5. Conclusion

_____

Summary

The current state of GDPR implementation via cookie-banners centers on legalese rather than interactive, usable graphical elements. This creates challenges even for privacy-aware designers and underscores the siloization of knowledge about cookie banners and consent. Our qualitative interviews with practitioners implementing cookie banners did not produce our expected narrative: that business pressure forces designers and front-end implementers to find ways to shape the banner for compliance, while cunningly bypassing meaningful consent to collect profitable data. Instead we heard how attitudes towards compliance and a fixation on legalese over user-experience (whether designing to deceive, or designing for meaningful consent) shape the cookie banner ecosystem. There is progress in incorporating language requirements as part of data privacy laws, but there is a long way to go.

Building on our findings, we proposed an initial framework of personas capturing attitudes towards graphical GDPR implementation. Using the personas to evaluate available consent management providers — from paid premium services to open source code repositories — a clear opportunity arose for how to better support a particular persona type: Discussers. Discussers engage across internal teams, attempting to find the balance of legally compliant language and user-friendly design. Some may not have large corporate budgets or deep technical knowledge, and typically the compliance team will “win,“ but an interest in engaging in dialogue about how to implement consent-based GDPR policies effectively and meaningfully is essential. Educational resources, conversational tools, contextual examples and best practices to shape discussions and cross-department collaboration would be especially helpful for those eager to discuss and find a balanced cookie banner solution.

Additional research is needed to understand how widespread are our initial findings of the challenge of legalese and jargon in cookie banner discussions.

Because our research included only designers and front-end developers, there are gaps in our understanding. In order to test and expand on these initial findings, future research should include interviewing both lawyers and designers to assess collaboration, surveys to get broader insights, or journey mapping the implementation process with participants. Another key opportunity would be to interview business executives and managers, as participants ultimately responded to and accommodated requests from these stakeholders.

Going forward

Providing better support to people engaging in data consent conversations is essential to expand the conversation and include more stakeholders, which are prerequisites to protecting user privacy and shifting power to make informed consent actionable. Stakeholders would benefit from vetted, free resources guiding conversation and knowledge-sharing across designers and compliance professionals. Open repositories cataloging best practices and examples for policy design implementation in different contexts would be especially useful both as templates to fork, and as conversation starters.

Ideally, informed and meaningful consent will in time become the norm, but examples must be made. The status quo of GDPR and other data consent policy implementation through consent-based cookie banners does an unacceptably poor job of this, as our research has proven. Since the launch of GDPR in 2018, data protection has been largely considered a specialized subject not relevant or shaped by most audiences. However; the tide is shifting. In California, updates to the CCPA – expanding the opt out rights and establishing a regulatory authority, among other changes – were established via Proposition 24. While aspects of the CPRA are controversial among the privacy advocacy community, this direct vote on the subject signals that its data privacy is now a public issue with momentum. Significantly, updated regulations to CCPA effective as recently as March 2023 provide opt-out language requirements for consumer clarity and comprehension. Similarly, more and more policies now call out dark patterns as an unacceptable practice.

To conclude, we present a provocation. Despite repeated exposure to cookie banners while using the web, non-professional website managers and casual content creators should not be expected to have working knowledge of GDPR and consent. This stands in stark contrast to payment processing, a no less technically demanding domain governed by a complex set of regulations. Despite the complexity, specialized domain knowledge is not required to integrate payment processing on websites. Drag-and-drop website builders such as Squarespace offer multiple options. Walking through the path of search query to successful payment implementation is far more straight-forward than navigating cookie banners.

We propose that the financial services industry could be a source of analogous inspiration for GDPR and other data privacy law implementation on user interfaces. The directly aligned incentives for easy commercial transactions have set better benchmarks for how to implement policies for financial processing online. We aren't faced with complex legalese every time we make an online payment (that is reserved for the Terms & Conditions). Instead, the ecosystem has produced innovative design elements that implement consumer protection policies by centering the end user's experience and needs.

Implementing consent-based data collection policies via graphical, user-facing interfaces urgently needs a more human-centered user experience approach. We hope that this preliminary research can bring more stakeholders to the table, and help provide a foundation for educational resource development. These are critical steps in shifting data privacy policy implementation out of an ethos of mere compliance toward active multi-stakeholder dialogue grounded in user experiences. Policy compliance and seamless, informative user experience do not have to be at odds. In fact, they are the formula for meaningful consent design.

Part 6. Bibliography

_____

A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang, S. Wilson, “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online,” *ACM Comput. Surv.*, vol. 50, no. 3, pp. 1–41, May 2018, doi: 10.1145/3054926.

California Privacy Protection Agency. “California Consumer Privacy Act Regulations.” *CA.gov.* March 29, 2023. https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

C. Gray, C. Santos, N. Bielova, M. Toth, D. Clifford, “Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective | Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems,” *ACM Conferences*. https://dl.acm.org/doi/abs/10.1145/3411764.3445779.

C. Matte, N. Bielova, and C. Santos, “Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe’s Transparency and Consent Framework,” November 2019, doi: 10.48550/arXiv.1911.09964.

C. Pershan and C. Sinders. “Why Europe’s Digital Services Act Regulators Need Design Expertise,” *Tech Policy Press, December 12, 2022. https://techpolicy.press/why-europes-digital-services-act-regulators-need-design-expertise/*

C. Santos, A. Rossi, L. Sanchez Chamorro, K. Bongard-Blanchy, R. Abu-Salma “Cookie Banners, What’s the Purpose? | Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society,” *ACM Conferences*. https://dl.acm.org/doi/abs/10.1145/3463676.3485611

C. Santos, N. Bielova, C. Matte, “Are cookie banners indeed compliant with the law?” in *Technology and Regulation*. https://techreg.org/article/view/10990.

C. Sinders, “Designing Against Dark Patterns,” *GMFUS*. https://www.gmfus.org/news/designing-against-dark-patterns.

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*, London United Kingdom, November 2019, pp. 973–990. doi: 10.1145/3319535.3354212.

D. Stauss and S. Weber on March 16, 2022 “How do the CPRA, CPA & VCDPA treat dark patterns?,” *Byte Back*, March 16, 2022. https://www.bytebacklaw.com/2022/03/how-do-the-cpra-cpa-and-vcdpa-treat-dark-patterns/.

Electronic Privacy Information Center. “California’s Proposition 24” EPIC.org. N.D. https://epic.org/californias-proposition-24/

E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, E. P. Markatos, “User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users | Proceedings of the Web Conference 2021,” *ACM Conferences*. https://dl.acm.org/doi/abs/10.1145/3442381.3450056

European Data Protection Board. “EDPB adopts Guidelines on Art. 60 GDPR, Guidelines on dark patterns in social media platform interfaces, toolbox on essential data protection safeguards for enforcement cooperation between EEA and third country SAs.” *Edpb.europe.eu.* March 15, 2022. https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-art-60-gdpr-guidelines-dark-patterns-social-media-platform_en

The European Data Protection Board. “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.” *Edpb.europe.eu.* October 20, 2020. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

European Union. “Digital Services Act.” *EUR-Lex.* October 27, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, “A Design Space for Effective Privacy Notices,” in *The Cambridge Handbook of Consumer Privacy*, 1st ed., E. Selinger, J. Polonetsky, and O. Tene, Eds. Cambridge University Press, 2018, pp. 365–393. doi: 10.1017/9781316831960.021.

J. M. Bauer, R. Bergstrøm, R. 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*, vol. 120, p. 106729, July 2021, doi: 10.1016/j.chb.2021.106729.

J. King and E. MacKinnon. “Do the DSA and DMA Have What It Takes to Take on Dark Patterns?” *Tech Policy Press,* June 23, 2022. https://techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/

J. Luguri and L. J. Strahilevitz, “Shining a Light on Dark Patterns,” *Journal of Legal Analysis*, vol. 13, no. 1, pp. 43–109, March 2021, doi: 10.1093/jla/laaa006.

K. Gupta, “Toward a future of trusted design: our recommendations to the European Data Protection Board,” *World Wide Web Foundation*, May 06, 2022. https://webfoundation.org/2022/05/toward-a-future-of-trusted-design-our-recommendations-to-the-european-data-protection-board/

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*, April 2020, pp. 1–13. doi: 10.1145/3313831.3376321.

M. von Grafenstein, J. Heumüller, E. Belgacem, T. Jakobi, P. Smieskol, “Effective regulation through design – Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking technologies in personalised internet content and the data protection by design approach,” *ResearchGate*.

https://www.researchgate.net/publication/355394794_Effective_regulation_through_design_-_Aligning_the_ePrivacy_Regulation_with_the_EU_General_Data_Protection_Regulation_GDPR_Tracking_technologies_in_personalised_internet_content_and_the_data_protectio

N. Arvind, M. Arunesh, C. Marshini, and K. Mihir, “Dark Patterns: Past, Present, and Future,” *Queue*, April 2020, doi: 10.1145/3400899.3400901.

Ø. H. Kaldestad, “Report: Deceived by Design : Forbrukerrådet.” https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

O. Radley-Gardner, H. Beale, and R. Zimmermann, Eds., *Fundamental Texts On European Private Law*. Hart Publishing, 2016. doi: 10.5040/9781782258674.

P. Graßl, H. Schraffenberger, F. Z. Borgesius, and M. Buijzen, “Dark and Bright Patterns in Cookie Consent Requests,” *jdsr*, vol. 3, no. 1, Art. no. 1, February 2021, doi: 10.33621/jdsr.v3i1.54.

The European Parliament and Council. “REGULATION (EU) 2016/679 ... 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.” *Official Journal L 119/1.* *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679*

S. Rieger and C. Sinders“Dark Patterns: Regulating Digital Design,” May 13, 2020. https://www.stiftung-nv.de/en/publication/dark-patterns-regulating-digital-design

Appendices

_____

Appendix A. Interview questions

Background

1. Tell us about your role.

a. You do NOT need to speak as an employee, and we want you to be comfortable sharing your opinions and individual experiences knowing that it will not be traced back to you. Nobody will know where you work or that you spoke to us.

2. What other roles/background do you have that's relevant?
3. How big is your team? What roles are on it?

Pushing pixels and shipping product

1. What's been your experience with cookie banners? As a user, designer, manager?
2. How did you first learn about GDPR/CCPA?
3. When is the first time you heard about it at work?

a. Or a memorable time?

4. How were you tasked with implementing the policy?

a. What role did you play specifically?

b. Did the direction come from management? What levels of administration were involved?

c. How was it framed?

5. Who was in charge of compliance? Is there a compliance department or person?
6. Walk us through how you began the process of designing the cookie banner (or working with designers)?

a. What did you call this?

7. What resources did you use to help support the design?

a. Did you already have a style guide or standards for buttons and things like that?

b. Who wrote the copy?

c. Who checked it?

8. Were there aspects of designing the implementation that were easy or no-brainers?

Managing conflict

What hard decisions were made? What key challenges did you face?

1. Were you ever asked to go against your design training or instincts to implement the policy in the design?
a. Talk us through an example, anonymize as much as you want.

Wrap-up

1. Do you want to take anything you said off of the record?
2. Anything else we should know?