Consent on the web : a transdisciplinary analysis

Michaël Toth

▶ **To cite this version:**

Michaël Toth. Consent on the web : a transdisciplinary analysis. Computers and Society [cs.CY]. Université Côte d'Azur, 2023. English. NNT : 2023COAZ4042 . tel-04259483

HAL Id: tel-04259483
https://theses.hal.science/tel-04259483

Submitted on 26 Oct 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITÉ CÔTE D'AZUR

ÉCOLE DOCTORALE
SCIENCES ET TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

THÈSE DE DOCTORAT

Le consentement sur le web: une analyse transdisciplinaire

Michaël TOTH

Centre Inria d'Université Côte d'Azur

Présentée en vue de l'obtention du grade de docteur en Informatique **d'**Université Côte d'Azur

Dirigée par : Nataliia BIELOVA, Chargée de recherche, Centre Inria d'Université Côte d'Azur

Co-dirigée par : Vincent ROCA, Chargé de recherche, Centre Inria de l'Université Grenoble Alpes

Soutenue le : 19 juin 2023

Devant le jury, composé de :

Serena VILLATA, Directrice de recherche, CNRS, Université Côte d'Azur

Zinaida BENENSON, Associate professor, University of Erlangen-Nuremberg, DE

Jean-François COUCHOT, Professeur, Université de Franche-Comté, Besançon

Nadezhda PURTOVA, Full professor, Utrecht University School of Law, NL

Arianna ROSSI, Chargée de recherche, Université du Luxembourg

LE CONSENTEMENT SUR LE WEB: UNE ANALYSE TRANSDISCIPLINAIRE

Consent on the web: a transdisciplinary analysis

Michaël TOTH

Jury :

Présidente du jury
Serena VILLATA, Directrice de recherche, CNRS, Université Côte d'Azur

Rapporteurs
Zinaida BENENSON, Associate professor, University of Erlangen-Nuremberg, DE
Jean-François COUCHOT, Professeur, Université de Franche-Comté, Besançon

Examinatrices
Nadezhda PURTOVA, Full professor, Utrecht University School of Law, NL
Arianna ROSSI, Chargée de recherche, Université du Luxembourg

Directrice de thèse
Nataliia BIELOVA, Chargée de recherche, Centre Inria d'Université Côte d'Azur

Co-directeur de thèse
Vincent ROCA, Chargé de recherche, Centre Inria de l'Université Grenoble Alpes

---

Université Côte d'Azur

Michaël TOTH

Le consentement sur le web: une analyse transdisciplinaire

x+132 p.

Ce document a été préparé avec LaTeX2e et la classe `these-ISSS` version v. 2.10.

Impression : output.tex – 9/10/2023 – 9:51

Révision pour la classe : these-ISSS.cls,v 2.10 2020/06/24 14:16:37 mpelleau

Le consentement sur le web: une analyse transdisciplinaire

Résumé

Le développement numérique des trois dernières décennies a transformé nos vies. Il a permis aux gens de partager des informations dans le monde entier, mais a également mis en lumière des risques sans précédent pour la vie privée. La généralisation de la publicité personnalisée comme moyen de financement des sites web est rapidement devenu un point de tension dans le domaine du droit à la vie privée. Les évolutions législatives dans l'Union européenne depuis 2008 ont posé certains fondements essentiels, en particulier l'importance centrale du consentement de l'utilisateur, conduisant au développement de plateformes de gestion du consentement (CMPs). Dans cette thèse, nous avons commencé par mettre en lumière la complexité des interfaces offertes par les CMPs, et les problématiques soulevées par certains types de designs spécifiques, généralement regroupés sous le nom de "dark patterns". Pour ce faire, nous avons mobilisé une méthode dédiée, la critique des interactions, pour réfléchir spécifiquement à trois types de design : le *cookie wall*, le *consent wall*, et le *service restreint*. Pour chacun d'entre eux, nous avons analysé les différentes phases de la gestion du consentement, et souligné l'intérêt d'un dialogue transdisciplinaire entre droit, informatique, et design. D'un point de vue juridique, nous avons analysé le rôle des CMP au regard du Règlement Général sur la Protection des Données (RGPD). En comparant les traitements de données effectués par plusieurs CMPs populaires, nous avons identifié les situations dans lesquelles ces entreprises définissent les finalités et les moyens des traitements de données, ce qui en fait de facto des responsables de traitement au sens de la règlementation européenne. Cela a d'importantes implications en termes de responsabilité pour ces entreprises. Enfin, nous avons analysé systématiquement la manière dont les CMP pouvaient influencer, contraindre ou manipuler les éditeurs de sites web par le biais de choix malhonnêtes en matière d'interface et de conception. En suivant le parcours d'un éditeur souhaitant installer les services de CMPs populaires, nous avons réalisé une analyse approfondie du processus requis, des options et des fenêtres contextuelles de consentement fournies. Nous avons mis en lumière les impacts, positifs et négatifs, de ces services, ainsi que leur influence potentielle sur les éditeurs de sites web.

Mots-clés : traçage, RGPD, ePrivacy, données personnelles, consentement, manipulation, dark patterns.

Consent on the web: a transdisciplinary analysis

Abstract

The digital development from the last three decades has transformed our lives. It enabled people to share information all over the world, but also brought to light unprecedented privacy risks. The widespread development of personalised advertising as a way to fund websites quickly became a point of tension in the area of privacy rights, and legislative developments in the European Union since 2008 have laid down certain essential foundations, in particular the central importance of user consent, leading to the development of Consent Management Platforms (CMPs). In this thesis, we started by shedding light on the complexity of the interfaces offered by CMPs, and the issues arised by certain specific types of designs, usually grouped under the name of "dark patterns". To this end, we have mobilised a dedicated method, interaction criticism, to reflect specifically on three types of designs: the *cookie wall*, the *consent wall*, and the *reduced service*. For each of them, we analysed the different phases of consent management, and highlighted the interest of a transdisciplinary dialogue between technical and social sciences. From a legal viewpoint, we have also analysed the role of CMPs with regard to the General Data Protection Regulation (GDPR). By comparing the data processing carried out by several popular CMPs, we have identified situations in which these companies defines the purposes and means of data processing, making them de facto Data Controllers in sense of the European regulation. This has important liability implications for these companies. Finally, we systematically analysed how CMPs could influence, coerce, or manipulate website publishers through dishonest interface and design choices. By following the journey of a publisher who wanted to install the service of popular CMPs, we realised an in-depth analysis of the required process, options, and consent pop-ups provided. We shed light on both positive and negative impacts of these services, and on their potential influence on website publishers.

Keywords: tracking, GDPR, ePrivacy, personal data, consent, manipulation, dark patterns.

Acknowledgements

This thesis would not have been possible without the help of many people to whom I would like to express my thanks, respect and gratitude. Rather than draw up an exhaustive list, I would like to say a few words to different groups of people, without necessarily naming them explicitly.

First of all, I would like to thank my thesis supervisors, Nataliia Bielova and Vincent Roca, for their patience, expertise and essential support during these four years. Thank you for believing in me and offering me this PhD position ! Thank you for your trust, for your sound advice, for your follow-up, for your dynamism, your availability and your many suggestions for improvement concerning the thesis and the articles, combined with a great organisational freedom, as well as for all your scientific and administrative work. I am extremely grateful to you for always supporting me with kindness and always giving me the time I needed to pass on your knowledge and expertise.

I would also like to warmly thank Zinaida Benenson and Jean-François Couchot who did me the honour of agreeing to review my thesis manuscript, as well as Nadezhda Purtova, Arianna Rossi, and Serena Villata, for agreeing to be part of my jury. Thank you for all your pertinent comments on my work.

Thanks to all my coauthors, and also to the reviewers of the PETS, CHI and APF conferences for sharing their ideas and their insightful comments to improve the published scientific papers.

To all my colleagues and former colleagues in the Privatics team, whether doctoral and post-doctoral students, interns, engineers, or permanent researchers, thank you for all the big and small discussions in the office and in the cafeteria, and for all your advice, both scientific and human. Thank you for making my integration so easy and enjoyable ! I would like to thanks particularly Helen Pouchot, our team assistant, for all your attention and for helping me to manage the numerous and interminable administrative procedures, and also Cristiana Santos, our external collaborator. Thanks for your availability, your professionalism, your invaluable help in writing articles and your support in difficult moments. It was a real pleasure working with all of you.

In addition, I would like to thank all my colleagues from other teams and services at the Inria research centres of Grenoble Alpes and Côte d'Azur universities, particularly the Moex and Indes teams, for their warm welcome, their help, and for all the constructive discussions. I would also like to thank the Inria Learning Lab members for inviting me as a MOOC assistant, which was the starting point of this adventure.

I would like to thank my mother, both for her material help and for encouraging me to continue my journey despite some complicated moments.

I would particularly like to thank my friend Emmanuelle. Thank you for encouraging me to go back to university, for your constant support during the nearly four years of my PhD, for your

proofreading of my thesis manuscript, for the close relationship we've had for nearly fifteen years and for all the fun times we've had together. Thank you for all the times you found the right words to help me keep hope alive and move forward. Thank you for being this extraordinary person who enriches my life simply by being there.

Finally, I'd like to thank my friends and acquaintances from the universities and sports and cultural associations I've attended, my flatmates, and all those who have helped and supported me in one way or another during this period.

This thesis would never have existed without all of you.

For all of that, I am eternally grateful.

Contents

Definitions

AEPD	Agencia Española de Protección de Datos (Spanish DPA)
ATP	Ad Tech Provider (Google list of advertisers)
BEUC	Bureau Européen des Unions de Consommateurs
CCPA	California Consumer Privacy Act
CJEU	Court of Justice of the European Union
CMP	Consent Management Platform
CNAME	Canonical Name (DNS record)
CNIL	Commission Nationale Informatique et Libertés (French DPA)
DPA	Data Protection Authority
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ePD	ePrivacy Directive
GA	Google Analytics
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
GTM	Google Tag Manager
GVL	Global Vendors' List
HCI	Human-Computer Interaction
IAB	Interactive Advertising Bureau
ICO	Information Commissioner's Office (UK DPA)
IETF	Internet Engineering Task Force
NCC	National Consumer Council
NOYB	"Not your business" (privacy activist NGO)
PETs	Privacy Enhancing Technologies
RTB	Real-Time Bidding
SEO	Search Engine Optimisation
TCF	Transparency and Consent Framework
TMS	Tag Management System
UA	Universal Analytics
UI	User Interface
UX	User Experience
Art. 29 WP	Article 29 Working Party
WTT	Web Tracking Technologies

CHAPTER 1

Introduction

Over time, the technological evolution has transformed our lives. In particular, over the three last decades, the development of digital technology [1] and its widespread penetration into every aspect of our life have led to significant advances in the diversity of information, facility of communication, and the speed and fluidity of exchanges. The Internet has long been seen as the ultimate means of emancipation, in the same way as the advent of writing or printing. But digital development has also increased the risks to people's privacy. The growth of online business and advertising has led many organisations to turn to funding based on the exploitation of personal data.

HTTP cookies first appeared in 1994, initially to allow the storage of a virtual shopping cart. They quickly evolved into a tool for tracking users. As early as 1997, recommendations were made by the Internet Engineering Task Force (IETF) to address the related privacy risks. In 1998, Google based its business model on the exploitation of personal data : providing its online search service without asking for payment from its users, it monetised the information collected about them to enable its advertisers to optimise their advertising campaigns [2]. In 2004, Mark Zuckerberg founds Facebook, which will soon engage in the path of personalised marketing fuelled by personal data [3]. The switch from contextual advertising to targeted advertising began around 2005, with the creation of dedicated Real-Time Bidding platforms such as DoubleClick Ad Exchange [4] (Google bought DoubleClick on 2007 and launched DoubleClick Ad Exchange in 2009). In 2009, in response to the growing prevalence of online tracking, the European institutions amended the ePrivacy Directive, prohibiting access to or storage of information on user terminals without consent [5]. As a result, the online advertising industry started to display a cookie information notice on websites. This notice evolved with years to become the ubiquitous consent pop-ups we all know. However, the text and design of these pop-ups are often manipulative, such as numerous interfaces in the web economy [6]. In 2010, Brignull [7–9] collected examples of manipulative or obstructive web designs under the name "dark patterns". His classification was later expanded and completed by several other works [10–14].

As the digital economy grows, so does online tracking. Numerous studies have demonstrated the prevalence of tracking over the past decade [15–18]. The European Union's General Data Protection Regulation (GDPR) adopted in 2016 and enforced since May 25, 2018, defines the rules on valid consent in [19, Art. 4, 7]. Requirement for collecting consent on websites resulted in large-scale adoption of consent pop-ups also known as "cookie banners" that became increasingly popular among the EU-based websites in previous years. Providing a legally-valid consent request to website visitors is complex. For example, in 2020 Santos et al. [20] identified 22 requirements of valid consent on the web based on both technical and legal analysis. This complexity has led to the professionalisation of the provision of consent pop-ups by service providers, in the form of pop-ups, CMPs. However, these are far from perfect. They raise questions about the sincerity of their

interfaces, the validity of their consent collection, the associated transfers of personal data, and their legal role under EU regulations. This thesis aims to contribute to these essential questions.

1.1 Motivations and thesis outline

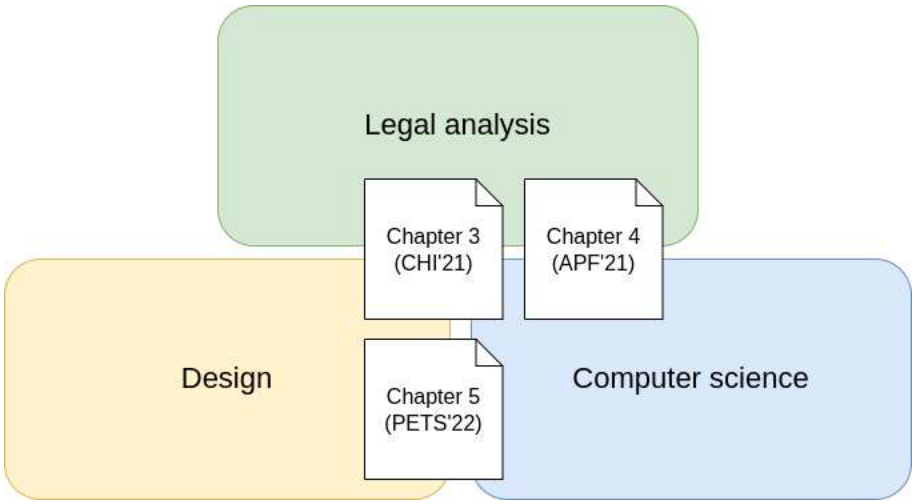


Figure 1.1 – Graphical depiction of the relation between chapters and their related topics.

The main object of this thesis is consent on the web. The overall objective is to analyse the tools and interfaces of the intermediation between the different actors of personal data collection on the web. This knowledge should allow us to offer paths for improvement in terms of privacy and personal data protection, and to achieve at least legal compliance with the requirements of European regulations. To achieve this goal, we study consent from transdisciplinary perspective, collaborating with legal and design scholars. Our contributions lay at the intersections of the fields as shown in Figure 1.1.

We focus in particular on the study of design choices in Consent Management Platforms (CMPs), and on their effect on website publishers and end users. We adopt as much as possible a transdisciplinary approach linking computer science, law, and design in order to encourage discussion and the emergence of new ideas.

This thesis contains three contributions preceded by a state-of-the-art, as described below. In Chapter 2, we start by reviewing various domains related to this work, from technical and legal knowledge on Web Tracking Technologies to user choices, and their manipulation.

Chapter 3 studies deceptive interfaces, or “dark patterns”. These are indeed widespread in the field of consent pop-ups. Their use circumvents the spirit of data protection regulations. We focus particularly on the study of three particular designs, the use of which can negatively impact the equal access to information on the web. We rely on the technique of interaction criticism to analyse the cross implications of designer, interface, user, and social impacts.

In Chapter 4, we look at the legal role of CMPs in the light of the GDPR. Indeed, CMPs are increasingly used. In the sense of the GDPR [19, Article 4 (7), 4 (8)], the companies providing CMP services generally define themselves as *Processors* instead of *Controllers*. This definition implies a processing of personal data realised on behalf of a *Controller* (in this case, the website

publisher) who "determines the purposes and means of the processing of personal data". However, we show that CMPs sometimes determine the means and purposes of the processing themselves, thus going beyond the role of Processor, and becoming de-facto a Controller. This legal role has important consequences for their responsibilities and obligations towards data subjects.

In Chapter 5, we look at the influence of CMPs on website publishers. We study how these actors, sometimes linked to digital marketing companies, shape the consent management interfaces according to their vision. By installing the solutions of several major CMPs on our own site, we highlight the presence of deceptive interfaces in certain configuration screens, which can lead to the deployment of non-compliant or manipulative solutions.

In Chapter 6, we finally conclude this work and open to several research perspectives. For instance, by doing a review of existing tendencies from the web advertising industry, we identify possible paths of evolution. We discuss perspective research, in particular regarding the new trend of server-side tracking. We analyse the advantages and risks of these changes, and we explore potential improvements of the situation regarding privacy, consent management, and the associated interfaces.

1.2 Contributions

This section summarizes the included published (Chapters 3 to 5) articles, precising the personal contributions for each.

1.2.1 Dark Patterns and the Legal Requirements of Consent Banners : An Interaction Criticism Perspective

Colin M. Gray, Cristiana Santos, Nataliia Bielova, ***Michael Toth*** *and Damian Clifford*

Our aim in this work is to shed light on common consent management interfaces impacting the freedom of access to websites : consent walls, tracking wall, and reduced service. We explore these designs through the lenses of HCI, design, privacy and data protection, and legal research communities, building upon previous work on "dark patterns" and deceptive design strategies. We perform an interaction criticism reading of three different types of consent pop-ups. We highlight the tensions and synergies that arise together in the act of designing consent pop-ups. We conclude with opportunities for dialogue across legal, ethical, computer science, and interactive systems scholarship to translate ethical concerns into public policy.

Statement of contributions I contributed by proposing a summarized version of the user journey across the consent process, and examples of manipulative designs, and to the tracking wall analysis. Also, I analysed the pattern of reduced choice architecture by applying the interaction criticism approach.

Impact This work has been cited in the following reports by regulators : UK Competition & Markets Authority report on Online Choice Architecture in 2022 [21] and Norwegian Consumer Council report in 2021 [22].

Appeared in *ACM CHI'21 : Conference on Human Factors in Computing Systems, May 2021, Yokohama, Japan / online (CORE2021 : A*).* Awarded Best of CHI Honorable Mention (top 5% of papers).

1.2.2 Consent Management Platforms under the GDPR : processors or controllers ?

Cristiana Santos, Midas Nouwens, ***Michael Toth****, Nataliia Bielova and Vincent Roca*

As European privacy regulations evolve, website publishers are increasingly turning to external providers, called consent management platforms (CMPs), to provide compliant consent management solutions. These solutions combine a consent pop-up displayed to site visitors, and storage of visitors' preferences usually in the form of a consent cookie in their web browser. CMPs often define themselves as data processors under the GDPR. In this work, by doing a legal and technical analysis of their different data processings, we identify situations where they can in fact become data controllers. We discuss the legal implications of these changes, and propose some recommendations to clarify their role.

Statement of contributions I contributed to the analysis of additional processing activities, scanning and pre-sorting of tracking technologies, included third-party vendors, and manipulative design strategies.

Impact Belgian Data Protection Authority used arguments presented in the paper in its decision to fine IAB Europe over its consent framework's GDPR violations [23]. European Union Agency for Cybersecurity (ENISA) has also cited this work in its 2022 report on Data Protection Engineering [24]

Appeared in : *Privacy Technologies and Policy – 9th Annual Privacy Forum, 2021, online (no known ranking).*

1.2.3 On dark patterns and manipulation of website publishers by CMPs

Michael Toth*, Nataliia Bielova and Vincent Roca*

Web technologies and services often collect personal data from users. In the EU, this collection requires user consent through the ePrivacy Directive (ePD) and the General Data Protection Regulation (GDPR). To comply with these regulations and integrate consent collection on their websites, website publishers often use third-party contractors, called Consent Management Platforms (CMPs), who provide consent pop-ups as a service. Previous research has shown that since the GDPR came into force in May 2018, the presence of CMPs has continuously increased. In our work, we choose to study the installation and configuration process of consent pop-ups and their potential effects on website publishers' decision making. To do so, we analyse the configuration process from ten services provided by five popular CMP companies. We identify the common unethical design choices employed and the manipulation of website publishers in favour of subscribing to paid CMP plans. We show that configuration options can lead to non-compliance,

while tracking scanners offered by CMPs can manipulate publishers. Our results demonstrate the importance of CMPs and the design space offered to website publishers, and we raise concerns about the privileged position of CMPs and their strategies to influence website publishers.

Statement of contributions As the first and main author, I contributed to the installation of the consent management solutions on the dedicated website, the analysis of the network communications of the services, the identification of unethical choices, and the scanner analysis.

Appeared in : *Proceedings on Privacy Enhancing Technologies Symposium, July 2022, Sydney, Australia / online (CORE2021 : A).*

CHAPTER 2

Background and related work

This chapter browses a state of the art for various related domains, from technical and legal knowledge on Web Tracking Technologies to user choices, and their manipulation. We start by a description of the major previous work in the field of third- and first-party tracking, and a focus on disguised trackers. In Section 2.2, we then review the legal context about the use of these technologies in the EU. Section 2.3 gives details about the de facto standard in consent management on the web, the Transparency and Consent Framework from IAB Europe. Finally, in Section 2.4, we list the main contributions of the academic community on manipulative design choices and web interfaces.

2.1 Web tracking technologies

2.1.1 Third-party tracking

HTTP cookies have been invented by Netscape developer Lou Montulli in 1994, to cope with the necessity to remember partial transactions from the visitors of an e-commerce web page. They were soon used as a tracking tool by advertising companies. Seeing the upcoming threat to privacy, the Internet Engineering Task Force (IETF) stated in RFC 2109 [25] in February 1997 that *"A user agent should make every attempt to prevent the sharing of session information between hosts that are in different domains"*. Since then, numerous works have studied tracking cookies and analytics tools. In 2009, Krishnamurthy and Wills [15] conducted a longitudinal study of the collection and aggregation of personal data of website visitors by third parties, highlighting a small number of actors in tracking ecosystem. In 2015, by analyzing third-party HTTP requests on the Alexa top 1 million sites, Libert [16] concluded that Google could track users on up to 80% of sites. In 2016, Englehardt and Narayanan [17] confirmed the extent of this tracking by conducting an automated analysis of stateful and stateless tracking in a large-scale analysis of 1M websites. Fouad et al. [18] crawled 84K pages to detect trackers by analyzing behavior of invisible pixels. They detected presence of invisible pixels on more than 94.51% of tested domains, showing the limitations of common privacy protections used by web browsers. As of today, third-party cookies are still commonly used as a web tracking technology. This state of things is likely to change in the near future, as :

— the population is becoming more educated about this use and the potential privacy implications for individuals and society [26] ;

— the legal framework already limits the use of tracking technologies, focusing in particular on third-party cookies, and DPAs are increasing their control activity [27] ;

— tracking and ad blockers are becoming widely used [26] ;
— many browsers already integrate protection from third-party cookies by default (Safari, Firefox, Brave) [28–30], and Chrome itself will start blocking them in 2024 [31].

To cope with the near-end of third party cookies, the industry is proposing alternative solutions, pushing towards first-party data sharing and the use of logged environments [32]. Companies also make use of browser and device fingerprinting [33] or IP based tracking [34] to track users without storing identifiers on their browser. Moreover, new techniques can help advertisers and trackers to disguise as first-parties, which we discuss in the following subsection.

2.1.2 Third-parties disguised as first-parties

As third-party cookies disappear, advertisers and tracking companies continuously adapt to keep their revenue. Since major privacy protection tools rely on blocking lists of third-parties [18], trackers can evade blocking if they are considered as first-party resources.

CNAME cloaking An evasion technique studied so far is the cloaking of tracking domains behind DNS canonical records ("CNAME"). It allows third-party tracking scripts to be considered as first-party ones, protecting them from being blocked by privacy protections. It has been extensively studied by Dimova et al. [35]. Web browser, such as Apple Safari [36] and Brave [37], and blocking extensions such as uBlock Origin [38] are already adapting their detection methods to protect from CNAME cloaking.

Server-side tagging CNAME cloaking is not the only way to disguise trackers. Tag Management Systems (TMS) have been used for years by marketing professionals to include and modify JavaScript in web pages without editing the code. Google Tag Manager (GTM) has become the most prevalent TMS on the market. A recent functionality of GTM, called server-side tagging, allows the trackers to execute outside of the execution context of the web browser, making it more difficult to block. This could make server-side tagging an efficient tool to hide trackers. To the best of our knowledge, no scientific study has analysed tag managers or GTM in particular, neither its client-side nor its server-side tagging version.

However, several people close to AdTech circles share their experience and publish screenshots and other analyses of these tools on the web, either to help publishers in their deployment or to point out legal or technical issues. They usually agree on how server-side tagging can increase performance on page load by reducing the amount of included resources, and increase publisher's control on data sent to third-parties. They also point out limitations, and highlight potential risks of data collection without user consent. This is, for instance, the opinion expressed by the IT and digital marketing expert Julius Fedorovicius in his howto on configuring server-side GTM [39]. He also noticed that server-side GTM can circumvent privacy protections, such as blocking extensions or Safari's ITP, and that a functional installation of server-side tagging GTM requires to pay for hosting and have a good technical knowledge. The analytics developer Simo Ahava, who tests and comments on new functionalities in Search Engine Optimisation (SEO) and digital marketing tools, maintains an extensive documentation on GTM [40]. In a recent article [41], he globally acknowledge that a switch towards first-party data collection can be a good evolution on the web, but expressed the same concerns as Fedorovicius' regarding the possible circumvention of privacy protections and ad/tracking blockers. He advocates for improving transparency and giving the choice to users. He gives some recommendations to improve transparency, such as developing a

server audit extension, publishing data processing documentation, and creating a dedicated signal similar to the Global Privacy Control (GPC) [42]. Other authors are even more pessimistic about server-side GTM, and think that it can make surveillance even worse than it is. The pseudonymous blog *Pixel de tracking* [43], who explores surveillance issues on the web, calls it a "Trojan horse for marketing teams" [44]. Sharing the opinion regarding the potential improvement of performances and security, the author(s) focus on the risk of circumvention of privacy protections, and suggest some improvement for blocking extensions, such as an improved detection of tracking JavaScript and URLs parameters, or IP-based blocking.

2.2 Legal requirements

As Web Tracking Technologies continue to evolve, regulators and policy makers try to ensure that the user's privacy is protected. Various legal sources were adopted in order to provide a framework for the collection and processing of personal data in the EU. We present below the most prominent ones, focusing on online tracking, end-user consent, and its legal validity. We first expose the binding legal sources, such as the European ePrivacy Directive (ePD) and General Data Protection Regulation (GDPR), and major decisions from the European Court of Justice (CJEU) and national Data Protection Authorities (DPAs). Then, we explore the non binding sources, such as DPA guidelines, as well as the best practices and DPA reports.

2.2.1 Binding sources : General Data Protection Regulation and ePrivacy Directive, and binding decisions

ePrivacy Directive The Privacy and Electronic Communications Directive 2002/58/EC (ePrivacy Directive or ePD) [45] was initially introduced in 2002 to address security and confidentiality in online services, complementing the Data Protection Directive 95/46/EC [46]. Seven years after its adoption, it has been amended by Directive 2009/136 [5]. The 2009 ePrivacy Directive requires to get prior consent before reading or writing operations on one's device. It covers all tracking technologies that either read/write or send information from user's device, including cookies, other browser storage, and also browser fingerprinting, unless being used *"for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network"* or *"strictly necessary in order to provide an information society service explicitly requested by the subscriber or user"* [5, Art. 5(3)]. ePD will eventually be repelled in the next years by a new ePrivacy Regulation, which is still under active discussion.

General Data Protection Regulation The General Data Protection Regulation 2016/679 (GDPR) [19] is the most important Regulation on privacy and data protection in the EU. Initially adopted in 2016, it came into force on 25th May 2018. The regulation formulates standards for the processing of personal data by affording rights to users (called "data subjects"), by imposing obligations for entities that process personal data (data controllers and processors), and a monitoring role for data protection authorities (DPAs). It applies to all processing of personal data by actors located in the European Economic Area (EEA), and for all individuals who are located in this area, and repeals the former Data Protection Directive 95/46/EC [46].

In the GDPR, natural or legal persons processing personal data are qualified as data controllers when they *"determine the purposes and means of the processing"*, or processors when they *"process personal data on behalf of the controller"* [19, Articles 4(7), 4(8)]. Personal data are defined

as *"[...] any information relating to an identified or identifiable natural person ('data subject') [...]"* [19, Article 4(1)]. Data controllers are required to ground their processing of personal data on one of six allowed legal bases [19, Art. 6]. The most common one is the consent of the data subject. Where consent is the chosen legal basis, the GDPR requires the collection of free, specific, informed and unambiguous consent from the data subject [19, Article 4(11)]. The burden of proof of such consent lies with the data controller [19, Recital (42)]. In the absence of a valid proof of consent, processing is unlawful unless the controller can demonstrate that another legal basis applies.

Decisions from the Court of Justice of the EU and from national DPAs In its 2018 decision following an on-site inspection, the French DPA (CNIL) ruled that the company "Vectaury" acting as a TCF CMP, failed to demonstrate a valid consent collection for an advertising processing of personal data, and did not comply with the transparency requirement regarding the purposes of processing [47, 48]. This interpretation has been contested by the IAB Europe [49]. The Belgian DPA conducted an investigation of the IAB TCF in response to 22 complaints [50] claiming GDPR infringements, such as not providing adequate rules for the processing of special categories of personal data, failed to fulfill its obligations under Article 12(1) of the GDPR and Articles 13 and 14 of the GDPR [19]. As of today, the investigation is still ongoing. The CJEU has limited the design options for consent banners : on October 2019, in the Planet49 case [51], the Court ruled that a pre-ticked checkbox could not satisfy the requirement for valid consent. National DPAs further have made decisions at a national EU Member State level regarding design of consent banners. For example, the French DPA (CNIL) considers that absence of reject option violates the legal requirements for valid consent, highlighting it in its 2022 decisions against Google [52], Facebook [53] and numerous orders to comply in 2021 [27]. Recently, DPAs also took position about the international transfer of personal data following the decision of the CJEU in the Schrems II case [54]. In February 2022, several DPAs have issued a compliance order to website publishers for the use of Google Analytics in violation of Article 44 of the GDPR [55]. The CNIL analysed the qualification of data transfers resulting from the use of Google Analytics. The CNIL concluded that websites using Google Analytics were realising international data transfers to the US, and that such transfers were done without the appropriate data protection level required by the GDPR. The CNIL concludes that website publishers should either implement a proxy that removes all personal data before transferring it to the US, or stop using US-based solutions.

2.2.2 Non-binding sources : Guidelines and reports issued by the EDPB and national DPAs

Guidelines and reports issued by the EU Data Protection Board In 2018, the GDPR has introduced an independent organisation called European Data Protection Board (EDPB) to replace the previous Article 29 Working Party (Art. 29 WP). The EDPB is mostly composed of representatives from each EU national DPA, and is in charge of the application of data protection regulations in the European Union [56]. In 2020, the EDPB issued its *Guidelines 05/2020 on consent under Regulation 2016/679* [57]. In this document, the EDPB states that *"access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored"*. In practice, this interpretation means the EDPB does not consider preventing users from accessing a website without acceptance of tracking (commonly known as "tracking walls") to be a valid form of consent request. Legally, the EDPB

considers this technique as an infringement of the requirement for free consent prescribed by the GDPR [19, Art.4(11), 7(4)]. In January 2023, the EDPB also issued a Report of the work undertaken by the Cookie Banner Taskforce [58] created in September 2021 to address more than 500 complaints sent by the privacy activist organisation NOYB on 31 May 2021 [59]. In this report, EDPB members agree on their interpretation of legal requirements regarding eight common practices encountered, including absence of reject buttons and withdraw icons, use of pre-ticked boxes, classification of consent-based cookies as essential, and deceptive design of consent pop-ups.

DPA guidelines specifically about CMPs Numerous DPAs provide guidelines and recommendations regarding consent and tracking. In practice, legally required consent is often provided to websites' owners by Consent Managements Platforms (CMPs), that are further discussed in Section 2.3. Only few DPA guidelines specifically discuss the service offered by these providers. In their 2021 Guide on use of cookies [60, 3.2.3 (c)], the Spanish DPA asserts that *"as long as CMPs comply with the requirements and guarantees [for obtaining valid consent], they shall be deemed an appropriate tool [...]"*. It recommends that CMPs "*must be submitted to audits or other inspections in order to verify that [...] requirements are complied with*". The Irish DPA [61] reiterates that CMPs should be careful to avoid non-compliant designs already settled in the binding case law (see Section 2.2.1, and emphasises their accountability and transparency obligations. The DPA focuses especially on the obligation for the publisher to keep a record of their types of personal data processing, and of the user consent obtained in accordance with the GDPR requirements [19, Article 30], even when using a CMP.

DPA reports about the IAB Europe Numerous CMPs implement the Transparency & Consent Framework (TCF) developed by the European branch of the advertising professional organisation, IAB Europe. The UK's DPA (ICO) [62] published a report on AdTech and Real-Time Bidding, studying both IAB Europe's TCF and Google's framework and concluded that the TCF lacked transparency and observed a systemic lack of compliance to their data protection requirements of the real-time bidding sector.

2.3 CMPs and web advertising ecosystem

CMPs are companies providing "consent management pop-ups as a service". These pop-ups are then added by website publishers on their pages to be compliant with European and similar data protection laws. CMPs often rely on a de facto standard, IAB Europe's Transparency & Consent Framework (TCF). This section regroups the previous works related to CMPs, IAB Europe, the TCF, and the other actors of online advertising ecosystem ("vendors", website publishers, and data subjects). We further discuss the relations between all such actions in Chapter 5.

2.3.1 Interactive Advertising Bureau (IAB)

The Interactive Advertising Bureau (IAB) is an organization of advertising professionals founded in 1996. Its purpose is to develop technical standards, provide training, and make lobbying for the advertising industry. The organization regroups 45 affiliated IAB groups in the world, including Europe. The European branch of the IAB, called IAB Europe, has developed a common framework called Transparency and Consent Framework (TCF) (currently on version 2.0). The goal of

the TCF is to salvage the massive data collection that fuels the advertising ecosystem, while being compliant with the new data protection laws. This framework provides the specification and guidelines for CMPs and advertising vendors. IAB registration as a CMP or vendor costs $ 2,000 per year, and enables the subscriber to be present in the TCF and use the standardized consent signal.

IAB Transparency and Consent Framework The first version of the TCF (v1.1) was released by the IAB Europe in 2018. Its successor (v2.0) appeared in 2019. Vendors is the term used by the IAB to describe third-parties requesting consent to personal data processing. They can be, for instance, advertising or analytic companies, data brokers, or ID providers. As of 4 April 2023, 809 vendors are registered in a global list by IAB Europe, called *TCF v2.0 Global Vendors List* (GVL) [63]. Numerous CMPs include by default the whole GVL in their consent pop-ups, resulting for the end-user to potentially consent for all the registered vendors rather than limiting her consent (when applicable) to the vendors present in the publisher's website, as demonstrated by Matte et al. [64] with their Cookie Glasses extension.

2.3.2 Research studies about IAB TCF

Since then, numerous research publications have shed light on TCF-based CMPs. We summarize below the key findings of the most relevant studies in the fields of qualitative evaluation of consent, and large scale measurements of consent pop-ups.

Qualitative evaluation of consent In 2020, Nouwens et al. [65] studied the presence of dark patterns in the UI of five popular CMPs according to UK data provided by the advertising company Adzerk (now renamed Kevel) [66]. They found almost 90% of consent pop-up didn't meet the minimal legal requirements, and the absence of a "refuse" button on the first layer of the consent pop-up increases positive consent. Additionally, Matte et al. [67] discuss the purposes and legal basis pre-defined by the IAB Europe and suggest that several purposes might not be specific or explicit enough to guarantee a valid legal basis, and that a large portion of purposes should require consent but are allowed by the TCF to be gathered on the basis of legitimate interest. In 2021, Human and Cech [68] built a theoretical framework to evaluate consent collection from five major tech companies — Google, Amazon, Facebook, Apple, and Microsoft — focusing on interactions, graphical design, and text. They noticed asymmetric design, hidden information, and unclear statements. They show the way these companies gather consent to be ethically problematic, and sometimes non GDPR-compliant. Finally, Santos et al. [20] performed an interdisciplinary analysis of the legal and technical requirements of consent banners under the GDPR and ePD, identifying 22 requirements from legal sources and both technical and legal experts to verify compliance of consent banner design. They explored ways to realize manual or automated verification of these requirements, aiming to help regulators, NGOs, and other researchers to detect violation of EU legislation in consent banner implementation. They also showed which requirements are impossible to verify at scale in the current web architecture, because of a lack of dedicated automatic tools and standards in cookie banner design.

Large-scale measurements of consent pop-ups From January 2018 until May, Degeling et al. [69] studied characteristics of 31 consent pop-up libraries including several ones provided by TCF-registered CMPs by installing them locally. They found that 62.2% of European websites displayed consent pop-ups in October 2018. The authors observed a 16% increase in consent

pop-ups adoption by website pre- and post-GDPR. Hils et al. [70] analyzed 4.2 million domains between June 2018 and 2020, showing how the rate of adoption doubled year over year as a result of compliance with the EU data protection regulation, and that CMPs are mostly used by moderately popular websites. Focusing on the programmatic signals rather than user behaviour, Matte et al. [64] analysed 28,257 EU websites and found that 141 websites register positive consent even if the user has not made their choice and 27 websites store a positive consent even if the user has explicitly opted out.

2.4 Dark patterns and influence of design choices on users

Research has shown that far from being neutral, the design of consent management tools was using techniques to drive people using it toward the choice wanted by the developer. In this section, we list the most important works regarding influence of design choices, and their application in the field of online privacy.

2.4.1 Definition of dark patterns

The concept of "Nudge" was popularised by Thaler and Sunstein in their 2008 book [71] as *"any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives"*. Thaler describes nudge as aiming *"to help people make better choices as judged by themselves"* and uses the word "sludge" for tactics that encourage self-harming behaviours [72]. The possibility to apply nudges to privacy was notably studied by Acquisti in 2009 [73]. In 2010, the designer and scholar Harry Brignull coined the term "dark pattern" to name such unethical choices architectures. He described a dark pattern as *"a user interface carefully crafted to trick users into doing things they might not otherwise do [...] with a solid understanding of human psychology, and [which] do not have the user's interests in mind"* [7]. Dark patterns include all deceptive (to mislead users by creating a false appearance), manipulative (to influence or control the action of users by using a subterfuge), coercive (to force users to perform an action), or obstructive (to prevent the action by causing unnecessary difficulties and delays) designs of a User Interface (UI), made to influence the decision of users in the interest of someone else. Brignull et al. identified a taxonomy of twelve different types of dark patterns and collected examples in their "hall of shame" website [9]. Multiple research studies emerged since 2010, proposing taxonomies and definitions of dark patterns in various contexts [10, 12, 74]. Regulatory bodies also became very interested in defining dark patterns in Data Protection and Consumer Protection domains [21, 75–78]. In 2023, these taxonomies and dark patterns definitions from academia and regulators have been regrouped in a draft ontology with high-, meso- and low-level dark patterns by Gray et al. [14].

2.4.2 Application to online privacy and consent

Policy and regulatory reports Various reports have analysed the presence of deceptive, manipulative, coercive, or obstructive design choices in consent pop-ups nudging users toward acceptance of online tracking. We briefly present below the most important relevant to our research. In 2018, the Norwegian Consumer Council (NCC) [79] analyzed how interface designs on Google, Facebook, and Windows 10 make it hard for users to exercise privacy-friendly options.

The CNIL [80], in its report *Shaping Choices in the Digital World*, proposes a non-exhaustive typology of potentially deceptive design practices which have a direct impact on data protection with a graphical representation [81]. The ICO [82] consider a cookie consent mechanism that highlight an "accept" option over a "reject' option as a non-compliant approach. The same holds if the reject option is located in a second layer and the agree option is available in the first layer. It calls this "nudge behaviour" which influences users towards the "accept" option.

Academic research work Several studies specifically focused on the presence of dark patterns in consent pop-ups. Kulyk et al. [83] performed an online survey on 150 participants, most without computer experience, about their perception of cookie banners, finding that cookie banners were often seen as a nuisance more than a useful information. In 2019, Utz et al. [84] measured how the design of consent pop-ups influence the behaviour of acceptation or denial of consent, showing that small UI design decisions can have a significant impact on people's choices, and that strategies such as *interface interference* (highlighting "Accept" button in a binary choice with "Decline") has a strong impact of whether they accept third-party cookies. Chromik et al. [85] discuss dark patterns of explainability, transparency and control, focusing on intelligent systems. They conclude that the legal right to explanation provided by the GDPR is not sufficient, and advocates for *"specific guidelines and standards"*. In 2020, Nouwens et al. [86] studied the impact of design choices regarding consent pop-ups, user interface nudges, and granularity of available consent options, finding less than 12% of the studied websites to be compliant with EU law. Soe et al. [6] collected consent pop-ups from 300 Scandinavian and English-speaking news services looking for manipulative strategies, and came to the conclusion that *"all employ some level of unethical practices"*. Machuletz and Böhme [87] set up a user study of post-GDPR consent banners with 150 German and Austrian students, showing a significant increase in consent when the highlighted default "Select all" button is present, with participants often expressing regret about their choice after the experiment. In 2021, Gray et al. [88] highlight connections between HCI, design, privacy and data protection on consent pop-ups, focusing on three different types of dark patterns. Luguri et Strahilevitz [13] did a large-scale experiment to compare the influence of "mild" and "aggressive" dark patterns on different categories of American consumers. They notably found "mild" dark patterns to generate less negative feelings. Mathur et al. [89] use the combined approaches of psychology, economics, ethics, philosophy, and law to formulate a general definition of dark patterns and their effects on users.

2.4.3 Privacy studies focusing on developers

While it was demonstrated that dark patterns manipulate end users, various research have considered web developers and website owners to be users as well. Researchers started considering developers to be end-users as well in the mid-2010s in usable security and privacy by looking at software developers' nudging and its potential impact on end-user privacy. In 2016, Acar et al. [90] studied how to apply usable security principles to developers to improve understanding of their attitudes, knowledge and priorities. They highlight the differences of perceptions and goals between developers and end-users, the secondary concern of security for users, and the counterproductive effect of the overabundance of security recommendations. In 2021, Tahaei et al. [91] conducted an online survey of 400 participants with prior experience in mobile application development, showing that developers' choices were influenced by the impact on revenue, user privacy

and the assumed relevance of ads to users. They also found that highlighting the privacy implication of ad personalisation in the options could increase their choice of non-personalised ads.

However, other professionals from different fields are involved in the process of designing, creating, and maintaining a website, who are not necessarily developers. This can include executive people from a website-owning company and external processors, such as, for instance, legal experts or marketing agencies. Our 2022 work on the manipulation of website publishers by CMPs [92] is inspired by this. It focuses on all the actors potentially involved in the process of adding a GDPR consent banner to a website.

CHAPTER 3

Dark Patterns and the Legal Requirements of Consent Banners : An Interaction Criticism Perspective

Colin M. Gray, Cristiana Santos, Nataliia Bielova, ***Michael Toth*** *and Damian Clifford*

Appeared in : ACM CHI'21 : Conference on Human Factors in Computing Systems, May 2021, Yokohama, Japan / online.

I contributed by proposing a summarized version of the user journey across the consent process and examples of manipulative designs, and to the tracking wall analysis. Also, I analysed the pattern of reduced choice architecture by applying the interaction criticism approach.

Abstract

User engagement with data privacy and security through consent banners has become a ubiquitous part of interacting with internet services. While previous work has addressed consent banners from either interaction design, legal, and ethics-focused perspectives, little research addresses the connections among multiple disciplinary approaches, including tensions and opportunities that transcend disciplinary boundaries. In this paper, we draw together perspectives and commentary from HCI, design, privacy and data protection, and legal research communities, using the language and strategies of "dark patterns" to perform an interaction criticism reading of three different types of consent banners. Our analysis builds upon designer, interface, user, and social context lenses to raise tensions and synergies that arise together in complex, contingent, and conflicting ways in the act of designing consent banners. We conclude with opportunities for transdisciplinary dialogue across legal, ethical, computer science, and interactive systems scholarship to translate matters of ethical concern into public policy.

3.1 Introduction

The language of ethics and values increasingly dominates both the academic discourse and the lived experiences of everyday users as they engage with designed technological systems and services. Within the HCI community, there has been a long history of engagement with ethical impact, including important revisions of the ACM Code of Ethics in the 1990s [1,2] and 2010s [3–5], development and propagation of ethics- and value-focused methods to encourage awareness of potential social impact [6–8], and the development of methodologies that seek to center the voices of citizens and everyday users [9–11]. In the past few years, everyday users have begun to become more aware of the ethical character of everyday technologies as well, with recent public calls to ban facial recognition technologies [12] and further regulate privacy and data collection provisions [13, 14], alongside critiques and boycotts of major social media and technology companies by employees and users alike [15, 16]. These kinds of technology ethics issues have also been foregrounded by new and proposed laws and regulations—in particular, the General Data Protection Regulation (GDPR) in the European Union [17] and the California Consumer Privacy Act (CCPA) in the United States [18]. These new legal standards have brought with them new opportunities to define unethical or unlawful design decisions, alongside new requirements that impact both industry stakeholders (e.g., " data controllers", "data processors", designers, developers) and end users.

Of course, HCI represents one of many disciplinary framings of technology ethics, with important parallel work occurring in other communities such as Science and Technology Studies (STS), Privacy, Ethics, and Law. As the ethical concerns present in technological systems and services become more apparent and widespread, others have called for a transdisciplinary engagement in conjunction with these other disciplinary perspectives to more fully address the complex intersections of technological affordances, user interactions, and near and far social impacts [19–23]. Recent work has sought to bridge some of these perspectives through the use of *dark patterns* as a theoretical framing, calling attention to a convergence of designer intent and negative user experience [24–30]. We seek to explicitly build upon these traditions and concepts in this work.

In this paper, we draw together perspectives and commentary from HCI, design, privacy and data protection, and legal research communities, building an enhanced understanding of how these perspectives might arise together in complex, situated, contingent, and conflicting ways in the act of designing consent banners. The GDPR [17] and the ePrivacy Directive [31] demand user consent for tracking technologies and this requirement has resulted in a range of different techniques, interaction approaches, and even inclusion of dark patterns to gain user consent [32–35]. Thus, we took as our starting point for this paper a collection of consent processes for websites accessible to EU residents, where each consent process was captured through screen recording. We then built on prior analysis of this dataset to identify several consent patterns which were distributed across the temporal user experience that include initial framing, configuration, and acceptance of consent parameters. We then used our shared expertise as authors in HCI, design, ethics, computer science, and law to analyze these design outcomes for their legality using prior legal precedent [17, 31], and their ethical appropriateness using relevant strategies from the dark patterns literature [25].

Our goal in this work is not to identify the breadth or depth of consent approaches, or even primarily to identify which of these approaches is most or least legally or ethically problematic. Instead, we use an *interaction criticism* [36] approach to analyze and reflect upon several common approaches to designing a consent banner from multiple perspectives : 1) design choices evident

in the consenting process artifact itself; 2) the possible experience of the end user; 3) the possible intentions of the designer; and 4) the social milieu and impact of this milieu on the other three perspectives. Using this humanist approach to engaging with technological complexity, we are able to foreground conflicts based on role and perspective; identify how legal, design, and ethical guidance frequently conflicts or lacks enough guidance; and provide an interactive framework through which future work might assess ethical and legal impact across temporal aspects of the consenting process. This approach results in a detailed analysis of four consent strategies from multiple disciplinary and role-based perspectives, leading to an overview of the consent task flow in alignment with legal consent requirements and the identification of instances where dark patterns strategies are used to manipulate the user into selecting options that are not in their best interest.

The contribution of this paper is three-fold. First, we use a combination of legal and ethics frameworks to evaluate different approaches to obstructing or manipulating user choice when consenting, providing a range of examples to inform future policy work and ethics education. Second, we explore our exemplars using an interaction criticism approach, adding an ethics-focused layer to critical accounts of interactive systems. Third, we argue for transdisciplinary dialogue across legal, ethical, computer science, and interactive systems scholarship to translate matters of ethical concern into public policy.

3.2 Related Work

3.2.1 Recent work on consent banners

The most closely relevant work on which we build our contribution in this paper is a surge of studies on consent banners, including work primarily stemming from a legal compliance perspective [37–41] or a dark patterns or "nudging" perspective [32–35,42,43]. We will briefly summarize several key studies and findings in this area.

3.2.1.1 Design choices that impact user behavior

In 2019, Utz et al. [43] conducted a field study on more than 80,000 German participants. Using a shopping website, they measured how the design of consent banners influence the behaviour of people acceptation or denial of consent. They found that small UI design decisions (such as changing the position of the notice from top to bottom of the screen) substantially impacts whether and how people interact with cookie consent notices. One of their experiments indicated that dark patterns strategies such as *interface interference* (highlighting "Accept" button in a binary choice with "Decline"), and *pre-selected choices* for different uses of cookies has a strong impact of whether the users accept the third-party cookies.

In their 2020 study, Nouwens et al. [32] performed a study on the impact of various design choices relating to consent notices, user interface nudges and the level of granularity of options. They scraped the design and text of the five most popular CMPs on top 10,000 websites in the UK, looking for the presence of three features : 1) if the consent was given in an explicit or implicit form; 2) whether the ease of acceptance was the same as rejection—by checking whether accept is the same widget (on the same hierarchy) as reject; and 3) if the banner contained pre-ticked boxes, considered as non-compliant under the GDPR [17, Recital 32]. In their results, they found less than 12% of the websites they analyzed to be compliant with EU law. In their second experiment, they

ran a user study on 40 participants, looking at the effect of 8 specific design on users' consent choices. They recorded an increase of 22 percentage points in given consent when the "Reject all" button is removed from the first page, and "hidden" at least two clicks away from this first page. Finally, they found a decrease of 8 to 20 percentage points when the control options are placed on the first page.

Machuletz and Böhme [42] set up a user study of post-GDPR consent banners with 150 students in Germany and Austria. Building upon with behavioural theories in psychology and consumer research, they evaluated the impacts of 1) the number of options displayed to the user, and 2) the presence/absence of a "Select all" default button in the banners, nudging the user toward giving a complete consent. They showed a significant increase in consent when the highlighted default "Select all" button is present, with participants often expressing regret about their choice after the experiment.

Soe et al. [33] performed a manual analysis of GDPR-related consent banners. They manually collected banners from 300 Scandinavian and English-speaking news services, looking for manipulative strategies potentially circumventing the requirements of the GDPR. Then, they analyzed the design of these banners, and "found that all employ some level of unethical practices". In their findings, the most common patterns were *obstruction*, present in 43% of the tested websites containing dark patterns, and *interface interference*, present in 45.3%.

3.2.1.2 Issues with compliance and detection

In their 2019 study, Matte et al. [34] focused on Consent Management Platforms (CMPs) implementing IAB Europe's Transparency and Consent Framework (TCF) framework. They analyzed consent stored behind the user interface of TCF consent banners. They detected suspected violations of the GDPR and ePrivacy Directive by running two automatic and semi-automatic crawl campaigns, on a total of 28,257 EU websites. Specifically, they studied 1) whether consent was stored before the user made the choice, 2) whether the notice offers a way to opt out, 3) whether there were pre-selected choices, and 4) if the choice that the user had made was respected at all. They found 141 websites registering positive consent before the user's choice, 236 websites that nudged users towards accepting consent by pre-selecting options, and 27 websites that storing a (false) positive consent even if the user had explicitly opted out. They also developed free and open-source tools to enable DPAs and regular users to verify if consent stored by CMPs corresponds to their choice.

Human and Cech [44] built a theoretical framework to evaluate consent collection from five major tech companies—Google, Amazon, Facebook, Apple, and Microsoft—focusing on interactions, graphical design, and text. They noticed asymmetric design, hidden information, and unclear statements. They show the way these companies gather consent to be ethically problematic, and sometimes non GDPR-compliant.

Finally, Santos et al. [40] performed an interdisciplinary analysis of the legal and technical requirements of consent banners under the GDPR and ePD, identifying 22 requirements from legal sources and both technical and legal experts to verify compliance of consent banner design. They explored ways to realize manual or automated verification of these requirements, aiming to help regulators, NGOs, and other researchers to detect violation of EU legislation in consent banner implementation. They also showed which requirements are impossible to verify in the current web architecture.

Summary. Prior work has evaluated the impact of interface design on consent banners and the decisions of users. These studies have primarily addressed : a) the computational detection of concrete design choices evident in source code ; b) the user impact of these design choices ; and c) the legitimacy of some of these design choices from a ethics, legal, or policy perspective. However, much of this work has occurred in silos, resulting in a disconnection of these design choices from the overall consent flow, or a lack of identification of the ways in which particular dark patterns might be connected to legal requirements and the user experience. In this paper, we build upon this gap in substantive transdisciplinary discourse, addressing a cross-section of legal, design, and technical expertise in relation to consent design choices and dark patterns.

3.2.2 Practitioner- and Academic-Focused Discussions of Ethics

Previous scholarship has revealed markedly different discourses regarding ethical concerns, with the academic community largely focused on arguing in relation to moral and ethics theory (e.g., [7, 8, 45]) and the practitioner community focused more on tangible and problematic practices (e.g., [19, 24, 26, 46]). While there has been substantial interest in ethically-focused design practices in the HCI community for decades, most of this work has been subsumed into one of three categories : 1) the development and maintenance of a code of ethics in the ACM, including relevant use of this code in education and practice [3–5] ; 2) the construction and validation of methods to support ethics-focused practice, most commonly within the methodology of Value-Sensitive Design (VSD ; [7, 45]) ; and 3) the use of practitioner-focused research to reveal patterns of ethical awareness and complexity [19, 21–23, 47–50]. Work on VSD has also included efforts across these categories that identify opportunities for implementation in design and evaluation activities [22, 51, 52] as well as broader engagement in ethics-focused argumentation, building connections from ethical and moral theories to HCI and Science and Technology Studies (STS) concerns (e.g., [53–57]). One particular source of interest that relates to the framing of this paper is a recent paper by Kirkham [20] that links ethical concerns with VSD and guidance from the European Convention on Human Rights ; [20] is one of few examples of legal, ethical, and HCI discourses coming together with the goal of informing HCI scholarship and guidance that may inform design practices.

The practitioner discourse regarding ethics has been more diffuse, representing an interest in ethics-focused work practices (e.g., Nodder's *Evil by Design* [58]), but perhaps the most vital conversations have emerged around the conceptual language of "dark patterns." This term was coined by Harry Brignull in 2010 to describe "a user interface carefully crafted to trick users into doing things they might not otherwise do [. . .] with a solid understanding of human psychology, and [which] do not have the user's interests in mind" [24]. Brignull identified a taxonomy [59] of twelve different types of dark patterns and collects examples in his "hall of shame," which has subsequently been built upon by Gray et al. [25], Bösch et al. [46], and Mathur et al. [29]. In 2016, Bösch et al. presented a classification of eight "dark strategies" [46], built in opposition to Hoepman's "privacy design strategies" [60], which uncovered several new patterns : *Privacy Zuckering*, *Bad Defaults* ; *Forced Registration* (requiring account registration to access some functionality) ; *Hidden Legalese Stipulations* (hiding malicious information in lengthy terms and conditions) ; *Immortal Accounts* ; *Address Book Leeching* ; and *Shadow User Profiles*. These patterns were later extended in an online privacy dark pattern portal [61] for the community to study and discuss existing patterns and contribute new ones. Mathur et al. [29] used automated techniques to detect text-based dark patterns, such as *framing*, in a set of ~53K product pages from ~11K shopping

websites. They found 1,818 occurrences of dark patterns, involving 183 websites and 22 third-party entities. They built a classification of these dark patterns, dividing them in 15 types and 7 categories, and a taxonomy of their characteristics. Finally, they made some recommendations to mitigate the negative effects of these deceptive techniques on users. In this work, we rely more specifically on the five dark patterns strategies proposed by Gray et al. [25], which include : *nagging*–a "redirection of expected functionality that persists beyond one or more interactions" ; *obstruction*–"making a process more difficult than it needs to be, with the intent of dissuading certain action(s)" ; *sneaking*–"attempting to hide, disguise, or delay the divulging of information that is relevant to the user" ; *interface interference*–"manipulation of the user interface that privileges certain actions over others" ; and *forced action*–"requiring the user to perform a certain action to access (or continue to access) certain functionality."

In other complementary work addressing dark patterns, scholars have described how dark patterns are perceived from an end-user perspective [62,63], how these patterns appear in non-screen-based proxemic interactions [27] and in mobile interactions [64], how these patterns can impact online disclosure [65], and how these patterns can be used to motivate design discourses and argumentation about ethics [66]. Finally, Chivukula and Gray [26,67] have recently shown how interest in dark patterns can reveal larger patterns of coercion and abuse in digital technologies, building on the popular subreddit "r/assholedesign" to define properties of an "asshole designer."

Summary. Previous work relating to ethics addresses a broad range of concerns, arguing from moral philosophy and professional ethics, engaging with complexity from the practitioner perspective, or some combination of these perspectives. We seek to connect these concerns in a transdisciplinary framing, better connecting practitioner and academic concerns about ethics within the context of legal and design concerns using the language of "dark patterns."

3.2.3 Legal scholarship on cookie banners and consent requirements

While legal scholarship infrequently intersects with work from the HCI community (see [20, 68] for rare examples connecting HCI to policymaking), literature from a legal perspective is vital to our understanding of what practices may be lawful or unlawful, and how these policies emerge and are then tested by the courts. To provide a basis for arguing from a legal perspective in this paper, we provide a brief summary of some of the key legislation and requirements dictated by GDPR, which ground our analysis of problematic consent banners in Section 3.4.

GDPR is the key pillar of the EU data protection framework, as supplemented by the ePrivacy Directive. In essence, the regulation formulates standards for the processing of personal data. Personal data are defined as *"[...] any information relating to an identified or identifiable natural person ('data subject') [...]"* (Article 4(1) GDPR). Processing is similarly broadly defined and amounts to any action undertaken with such information (Article 4(2)). The GDPR regulates the processing of personal data by affording rights to users (called "data subjects"), by imposing obligations of entities that process personal data (data controllers and processors), and a monitoring role for data protection authorities (DPAs).

GDPR introduces specific *principles relating to the processing of personal data* (Article 5 GDPR) which guide data controllers and processors in the interpretation of the rights and obligations. Of immediate importance for are the lawfulness, fairness and transparency principles (Articles 5(1)(a) GDPR) and the accountability principle (Article 5(2) GDPR). The processing of personal data requires one of the conditions for lawful processing to be satisfied (Article 6(1) GDPR), namely *consent*. The ePrivacy Directive stipulates that user consent is required for proces-

sing information through the use of tracking technologies (which includes cookies, (Article 5(3) of the ePrivacy Directive) *. Consent is commonly expressed through interface design elements in the form of a pop-up.

Table 3.1 presents a synthesis of the legal requirements for valid consent which stem from the GDPR, the ePrivacy Directive (ePD) and the Court of Justice of the EU (CJEU). Consent is defined in Article 4(11) and complemented by Articles 6 and 7 of the GDPR which states that for consent to be valid, it must satisfy the following elements : it must be "freely given, specific, informed and unambiguous." The controller is required to be able to demonstrate consent (Article 7(1) GDPR) keeping in mind that, in assessing the "freely given" definitional condition, rendering access to the service conditional on consent may invalidate the reliance on consent (Article 7(4) GDPR). In short, consent is required to be presented in a manner which is clearly distinguishable from other matters (Article 7(2) GDPR) and represent a meaningful choice as evidenced by the ability to withdraw consent (Article 7(3) GDPR).

Summary. Legal scholarship has not yet provided a threshold for the appropriateness of specific design patterns in consent banners, and which requirements for a valid consent are or are not respected in each case. Although some regulators have provided classifications of dark patterns applied to various practices which have been deemed unfriendly in terms of privacy impacts, these classifications have not qualified which dark patterns are potentially unlawful and which legal requirements are potentially violated in relation to these patterns. We seek to address this gap, focusing on a legal compliance perspective by analyzing the lawfulness of these dark patterns from the consent requirements side.

3.3 Our Approach

3.3.1 Researcher Positionality

We explicitly and intentionally framed this project—and our broader research collaboration—in relation to transdisciplinary scholarship that expands beyond any one of the authors' respective disciplines. As one effort to acknowledge the subjective positions from which our readings of each consent banner emerges, we include a brief description of our disciplinary expertise as a means of increasing the transparency of our research efforts [70].

The authors of this paper are researchers that engage in research, design, or development across the following domains :

— Bielova and Toth are computer scientists with expertise in web privacy measurement and privacy compliance ;
— Gray is an HCI and design researcher with expertise in UX, ethics, values, and dark patterns ;
— Santos and Clifford are legal scholars with particular expertise in EU Data Protection law.

These different areas of disciplinary expertise are frequently contested, working in silos, or are otherwise in conflict with concepts or guidance from other disciplinary perspectives. We use the concept of "dark patterns" as a primary example of our means of connection to each other as scholars, while also recognizing that the concept of dark patterns has been addressed separately within the research communities of HCI, Computer Science and Law, with varying degrees of impact and limited interdisciplinary effort. In this paper, we explicitly leverage our collective

∗. Only functional cookies which are used for communications and strictly necessary purposes are exempted of consent. See more detailed analysis of the scope of consent in Santos et al. [40, Section 4].

Requirements	Provenance in the GDPR, ePD, CJEU	Description
Freely given	Art. 4(11), 7(4) GDPR	Consent should imply a voluntary choice to accept/-decline the processing of personal data, taken in the absence of any kind of pressure or compulsion on the user
Specific	Art. 4(11) GDPR, CJEU Planet 49 [69]	Consent should be separately requested for each purpose
Informed	Art. 4(11) GDPR, 5(3) ePD, CJEU Planet 49 [69]	The user must be given clear and comprehensive information about what data is processed, the purposes and means for expressing consent
Unambiguous	Art. 4(11) GDPR, CJEU Planet 49 [69]	Clear and affirmative action of the user
Readable and accessible	Art. 7(2), Recitals 32, 42 GDPR	Consent request should be distinguishable of other matters, intelligible, accessible to the user, using clear and plain language, not unnecessarily disruptive to the use of the website

Table 3.1 – Legal requirements for a valid consent, provenance in the GDPR, ePrivacy Directive (ePD) and the Court of Justice of the EU (CJEU).

attempts as a research team to bridge disciplinary silos as a way of collectively discussing future transdisciplinary approaches to ethics, policy, design, and computer science. This paper was written over a period of almost nine months, involving numerous online calls where we engaged with the transdisciplinary complexity of this space, seeking both to find a "common ground"—where concepts from each of our disciplinary perspectives might find resonance—as well as identifying how the emergent findings that are present in our argumentation might point towards disciplinary advances in each of our respective areas, and how these might be productively brought together as an example of transdisciplinary scholarship for the HCI community.

3.3.2 Data Collection and Framing

Due to the argumentation focus of this paper, we relied upon data sources collected in previous projects to identify salient consent design choices to elaborate further. From 2019–2020, a subset of the authors collected a broad range of examples of consent banners, using screen recording software to capture the entire interaction flow required to fully consent in accordance with GDPR requirements. The screen recordings were made using desktop-class devices only, recognizing that mobile experiences themselves are an important space for future work, likely with different forms of pattern instantiation and sources of manipulation.

We based our analysis on a dataset of 560 websites accessible from the EU from French-, Italian- or English- speaking countries : France, UK, Belgium, Ireland and Italy, and `.com` websites from Matte et al. [34]. Each of these sites was detected automatically in this prior work as containing a consent banner that implemented IAB Europe Transparency and Consent Framework (TCF [71]). These 560 websites also belonged to 1,000 top Tranco [72] list, which indicates po-

pular websites of the top level domain (TLD) of the above-mentioned European countries (e.g., `.fr`, `.uk`, etc) and domain `.com`. From this dataset, we focused on locating a range of potentially manipulative design exemplars, using recorded videos or screenshots of the consent experiences to support a manual and collaborative analysis of their design and text. In total, we reviewed recordings from over 50 sites and extensively analyzed the design and users' means of interaction with the consent banners on these websites. While reviewing other recent and relevant literature on ethical issues in the design of consent banners (e.g., [32, 33, 42]), we identified four main phases in the consent task flow (Figure 3.1) :

1. the initial framing as a user enters the site ;
2. the presentation of configuration options to accept or select more precise consent options ;
3. the means of accepting the configuration options ; and
4. the ability to ultimately revoke consent.

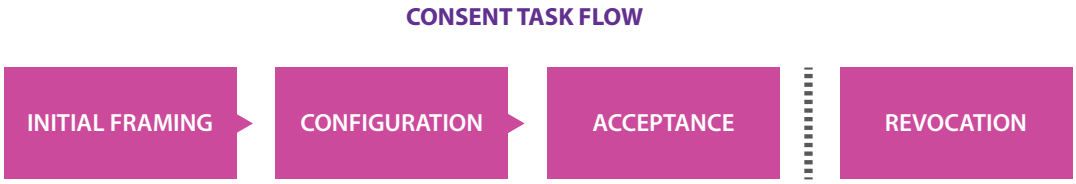


Figure 3.1 – The task flow of the consenting process by phase.

Within this task flow, we worked as a research team to identify four different combinations of design choices that were represented in the dataset and raised productive ethical dilemmas when viewed from multiple disciplinary perspectives. For instance, the consent types *reduced service* and *consent wall* we describe in the findings section of this paper had not previously been detected or precisely identified in prior work, either through empirical web measurements or from user studies. Moreover, EU Data Protection Authorities currently have conflicting opinions on the lawfulness of these practices that this analysis can clarify to policy makers [40] ; these opinions can only be derived from a legal, design, and computer science analysis of consent requirements and consent banners as we set out in the remainder of this paper.

Because our main goal in this paper is to examine the complexity of these design outcomes and not to identify how common these patterns occur "in the wild," we used the dataset as a source of inspiration and departure rather than as a means of conducting a content analysis or other inductive form of inquiry. We therefore focused on analyzing specific *types* of banners with the goal of representing a broad range of consenting approaches through our interdisciplinary perspectives rather than what was most typical or used on the most popular sites.

3.3.3 Data Analysis

Within each element of the task flow as embodied by a specific set of design choices, we inspected specific forms of manipulation through our analysis. We used the practice of *interaction criticism* [36] to investigate and interrogate manipulation from multiple perspectives. According to Bardzell [36], the practice of *interaction criticism* is the "rigorous interpretive interrogations of the complex relationships between (a) the interface, including its material and perceptual qualities

as well as its broader situatedness in visual languages and culture and (b) the user experience, including the meanings, behaviors, perceptions, affects, insights, and social sensibilities that arise in the context of interaction and its outcomes." The process of engaging in criticism builds upon four perspectives or positions of argumentation : 1) the designer ; 2) the interface itself ; 3) the user ; and 4) the social context of creation and use. In our work, we intend to build upon the practice of interaction criticism by highlighting the contributions of design scholarship, legal jurisprudence, and discussions of ethics and values from both academic and practitioner perspectives. Using this approach provided a conceptual means by which we could each intentionally de-center our own disciplinary expertise and vocabulary, foregrounding perspectives and concepts from other disciplinary traditions and subject positions in the search for common ground. Across these disciplinary perspectives, we sought to include a number of potential considerations :

1. the designer's potential intent in relation to the design choice ;
   potential considerations include : design judgments, context- or role-based limitations of the designer's work, means of balancing multiple constraints, use of design precedent
2. the designed interface itself ;
   potential considerations include : formal aspects of the UI, common design patterns that are exemplified by the interface under evaluation, indications of designed interactions or user experience inscribed into the interface, language used, typographic and compositional decisions, indication of feedforward
3. the perspective and experience of the end user ;
   potential considerations include : anticipated user interactions and experience, technical knowledge required or assumed of the end user, designer's perception of the system model
4. the potential social impact of the designed experience.
   potential considerations include : relevant business models and economic rationale, current and future role of technology, social acceptance or rejection of technology norms, agency of users and technology providers

Using this approach, we iteratively built out an argument from each of the perspectives listed above, seeking to identify salient design principles, potential social expectations or means of describing intent, and legal or policy guidance through which the consent design choices could be framed. Through this process, authors with expertise across a range of disciplinary perspectives added their own sources of evidence, while also reviewing the coherence of argumentation from other disciplinary perspectives. We used the qualitative/interpretivist notion of reflexivity to continuously identify strengths and gaps, seeking not to reach objective and final consensus, but rather to explore differences in disciplinary perspectives and the points at which these perspectives overlapped or collided.

3.4 Findings

We organize our findings based on the temporal direction of a user's task flow, investigating four design choices in relation to the consenting task flow. Revocation is the fourth element of the task flow, which we include in Figure 3.1 ; however, we do not address revocation in our analysis approach. Across these user consent tasks and criticism perspectives, we engage in an interaction criticism analysis over the following sections, particularly highlighting the interplay of legal requirements, potential violations, and possible gaps in legal and policy guidance. In

Figure 3.7 we summarize how this set of design choices relates to legal requirements and dark patterns strategies in the context of the overall consent task flow.

3.4.1 Initial Framing

The "initial framing," according to Figure 3.1, corresponds to the very first component of the consent mechanism a user sees when entering a website. This framing typically consists of an information banner disclosing the tracking technologies used and their purposes for data processing, with an acceptance button, and a link to the website's privacy policy. The initial framing banner can also take the form of a dialog or popover displayed on a part of the page, but may also completely block the page, preventing any action by the user until a choice has is made, such as the consent wall and tracking wall types that we analyze in the following sections.

3.4.1.1 Consent Wall

A consent wall is a design choice that blocks access to the website until a the user expresses their choice regarding consent. This design choice allows a user to select between acceptance and refusal; however, the concrete use of the website is blocked until a choice has been made. An example from the website of `https://www.bloomberg.com/europe` illustrates the use of a consent banner forcing the user to make a choice, thus blocking the access of the website, as shown in Figure 3.2 †.

We now consider this design choice from four different perspectives, in line with the interaction criticism perspective, overlaying our analysis with legal analysis and commentary regarding the implementation of dark patterns.

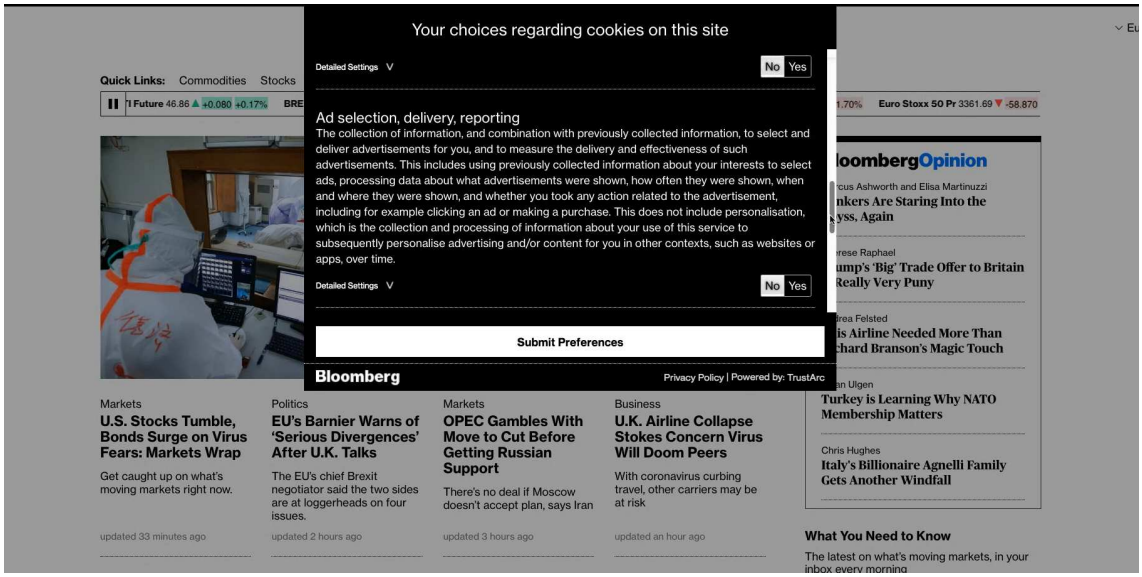


Figure 3.2 – An example of a consent wall, recorded on 5 March 2020. Credits : Bloomberg.com

†. Video recorded on 5 March 2020 : `https://mybox.inria.fr/f/28f689abbd8a4f188c89/`

Designer perspective The use of a consent wall clearly separates the consent process from the use of the underlying website, visually and also interactively. Thus, the actual presentation of the consent banner relies upon typical, while perhaps not fully ethical, interface design patterns. If from the *designer perspective*, the intent is likely to be read as reducing user choice through the layering and locking out of functionality, it could be deemed to be both manipulative and coercive. However, from a *legal perspective*, including a visual limitation—such as blocking access to a website until a user expresses a choice—will force the user to consent and therefore it possibly violates a *freely given* consent. Rendering access to a service conditionally based upon consent could raise serious concerns in relation to the 'freely given' stipulation in the definition of consent (Article 7(4) of the GDPR as further specified in Recital 43 thereof). In effect, one could take the view that this separation between a "consent request" *vis à vis* "content of the request" could be considered as being of strategic advantage to the designer, since the separation of these codebases—one mandatory and site-wide impacting the entire user experience, and another that is page-specific—might naturally lead to decisions such as a consent wall. Additionally, the designer/controller is required to be able to demonstrate consent (Article 7(1) GDPR) and to fulfill this requirement, consent must be presented in a manner which is clearly distinguishable from other matters, which may potentially support aspects of such interruption to the user experience and serve as a practical implementation of the obligations laid down by the Regulation. Although, we observe that such an interpretation would appear to subside in the face of a teleological interpretation of the GDPR. If the user's choice does not correspond to the expected choices of the website publisher/designer, the website should provide other means of accessing the same version of the website (such as paid options), where the user's choice is respected. A consent wall that blocks the service provided by the website without other options has detrimental effects.

User perspective A *user* demonstrates their intent to gain access to the content of a site by navigating to a particular URL or by clicking a link. This intent points to their desire to access the content of a website, and only after the site loads do they face obstructive overlays that are of secondary importance to many users beyond the content the user was intentionally navigating towards. In this way, the consent wall can be considered as a visual and interactive barrier to desired content, exemplifying the dark pattern strategy of *forced action,* defined as "requiring the user to perform a certain action to access [...] certain functionality." In addition, although this design choice allows some degree of accessibility or interaction, a consent wall could also be considered as an *obstruction* to the user's primary intention to access the full content of the website visited, with the relative weight or impact of this dark pattern of *obstruction* to be based on the amount of content or interactivity that is obscured or limited.

Interface perspective The manipulation evident in the designed interface is intentionally structured to achieve a higher collected number of positive consents from users through the use of layered strategic elements as popovers, lightboxed forms, and other means of layering content to encourage consent—and by comparison, discourage rejection. Notably, when content desired and deemed relevant to the user is not made immediately or readily accessible, and is instead hidden under an overlay or other interface elements, with the primary motivator *to disguise relevant information as irrelevant*, the interface decisions could also point towards the use of *obstruction* in placing visual and interactive barriers between the target of the user's interaction (the content) and the only salient interactive target provided by the site (the consent banner).

This design choice may violate another requirement named the "readable and accessible consent request" (Article 7(2)), meaning that a consent request should not be unnecessarily disruptive to the use of the service for which it is provided (Recital 32). Thus, it could be argued that consent walls are confusing and unnecessarily disruptive of the user experience, and other consent design implementations could be sought while engaging users. This legal evaluation of the interface decisions requires a more evidence-based assessment of what will amount to a concrete implementation of what is "unnecessarily disruptive." In fact, much depends on the context at hand—as experienced by the end user—but with these provisions in mind, it could be argued that although a consent wall may be a legitimate means of requesting consent, the user should also have the flexibility to cancel the request and continue browsing without the burden of tracking. Practically speaking therefore, compliance with this legal requirement of a freely given consent is *context dependent*.

Social impact perspective Positioning consent as the main mechanism to access desirable content could result in consent auto-acceptance or consent fatigue, where users tend to automatically dismiss any selection options in their path in order to achieve their goal. And it is this potential that demonstrates how the legitimacy of consent walls—from a legal perspective—is a complicated question. Across multiple websites, the immediate request for consent could take on the characteristics of the dark pattern "nagging"—which while not inherently harmful as a single case, gains strength through its ubiquity across multiple web experiences that may be experienced in a single web browsing session. Thus, the social relationship shown to be valued through the GDPR is one where the interruption of service may be seen as useful, or even necessary depending on the context at stake.

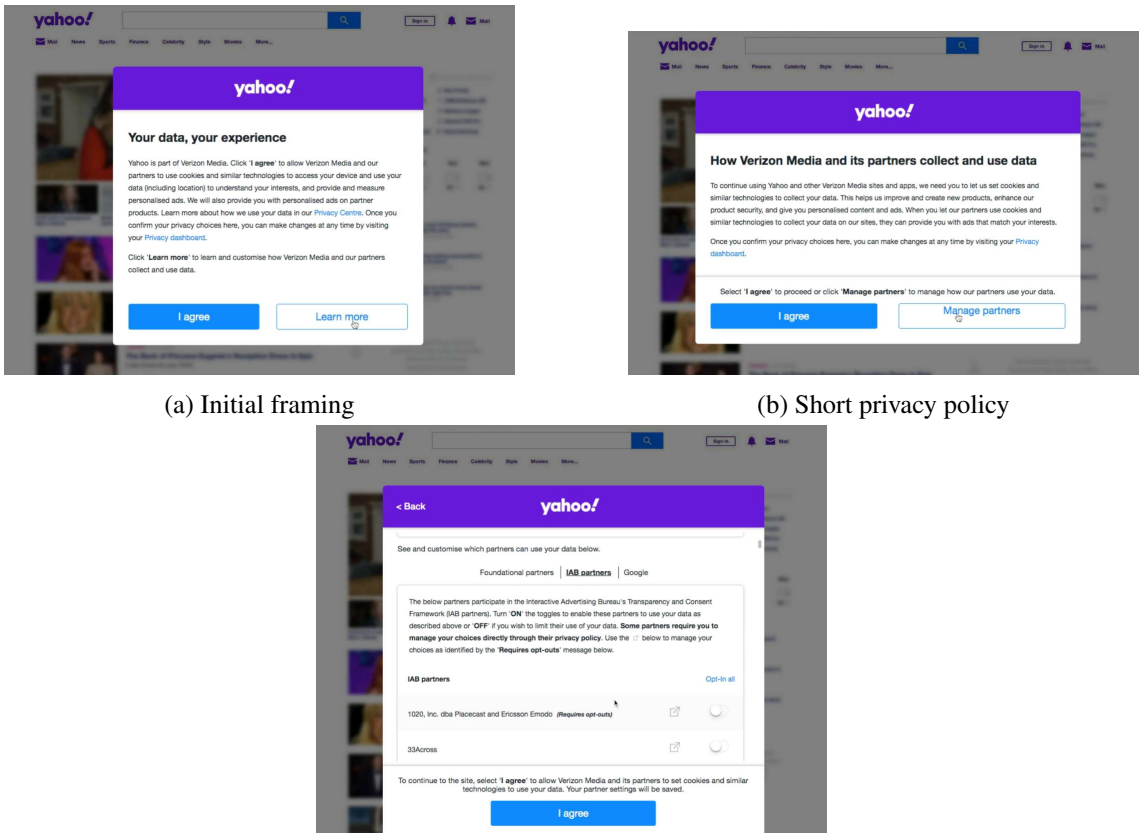
Summary This design choice presents a tension between i. interactive separation of user activities, ii. strategies meant to limit user interaction prior to completing the consenting process, iii. requirements that mandate that consenting precedes use, and iv. the various impacts of both a "burden of care" on the part of the designer and the "freely given" nature of the consent process itself. These tensions, while potentially pointing towards rejection of this design choice as legally acceptable, also show the diminished user experience and unnecessary fragmentation of the user experience in order to satisfy legal requirements.

3.4.1.2 Tracking Wall

A tracking-wall is an instance of a *consent wall*, however with more detrimental consequences to the user. In addition to blocking access to the website until the user makes their choice, a tracking wall gives the user only one option : to consent and accept any terms offered by the site, without any possibility to refuse. In the legal domain, a tracking wall is also called a "cookie-wall" or "take it or leave it" choice [73]. Differently from a *consent wall* (section 3.4.1.1), a tracking wall cannot result in a *reduced service* (section 3.4.2.1) because the only option the user has is merely to accept consent in order to access the website. An example of this design choice can be found on the website of `https://yahoo.com` which illustrates the use of a consent banner that provides only one choice—to accept—while blocking access to the website, as depicted in Figure 3.3 [‡]. Our interaction criticism analysis of consent walls provided in section 3.4.1.1 applies to the tracking

‡. Video recorded on 4 March 2020 : `https://mybox.inria.fr/f/6d9ea3b16c6b487d8065/`.

wall as well. In this section, we complement the consent wall analysis with additional specificity related to tracking wall design choices.



(a) Initial framing

(b) Short privacy policy

(c) Configuration

Figure 3.3 – Example of a tracking wall, recorded on 4 March 2020. Credits : Yahoo

Designer perspective When deploying a tracking wall in a website, a designer chooses to restrict a visitor's access to content or service when that visitor denies consent. Therefore, the only access possibility is complete acceptance of tracking technologies used by the website provider and/or their third-party partners, under any terms that may be provided explicitly, hidden, or simply left unstated. As a result, this design choice puts more aggressive pressure on the user's action, with even less respect of a freely given choice. It therefore raises the same questions as the consent wall regarding the legal requirement of a *freely given* consent.

Interface perspective The interface here is very similar to the one encountered when facing a consent wall. The only difference is the absence of a possibility to refuse consent. As shown in the example provided in Figure 3.3, some tracking wall examples do include a second informational button ("learn more"); however, even if present, these buttons typically do not provide immediate access to additional configuration options. The overall impact of this interface experience serves to obstruct access to any web resources except for the consent box, until the only real choice of "I agree" has been made.

User perspective A tracking wall represents a form of obstruction which prevents the user from achieving their intended action, such as reading an article, creating an account, logging in, or posting content. It interrupts the user browsing, giving them a single "choice" to give consent or to quit the website. The absence of any way of using a service/accessing a website without giving consent (e.g. via a "Refuse" or "Decline" option) makes the interface actively coercive, leading to an unpleasant experience for users who do not wish to give consent. Thus, beyond being obstructive, this lack of freely given consent may also constitute a form of forced action. From a legal perspective, the CNIL's Draft Recommendation on the use of cookies [74] proposes that consenting to trackers should be as easy as refusing them, and users should not be exposed to negative consequences should they decide to refuse consent to tracking.

Social impact perspective A tracking wall, from a website owner's point of view, could be a means to offset costs relating to providing the web service, facilitating a balancing of traffic with advertising revenues. Choosing to completely block the site has a greater impact than a consent wall, as it is likely to deprive part of the population of access to all the content or service. More specifically, this restriction may make privacy concerns incompatible with the use of a website not financed by the user, such as those financed by advertising. For instance, on information and news websites, this type of design choice may restrict access to information for users depending on their income. In the worst case, this could lead to significant disparities in accessing information and equality among individuals, with the wealthiest people falling back on paid sites without advertising. Paywalls do exist in some areas, they are generally reserved for content where there is a general social understanding of cost.

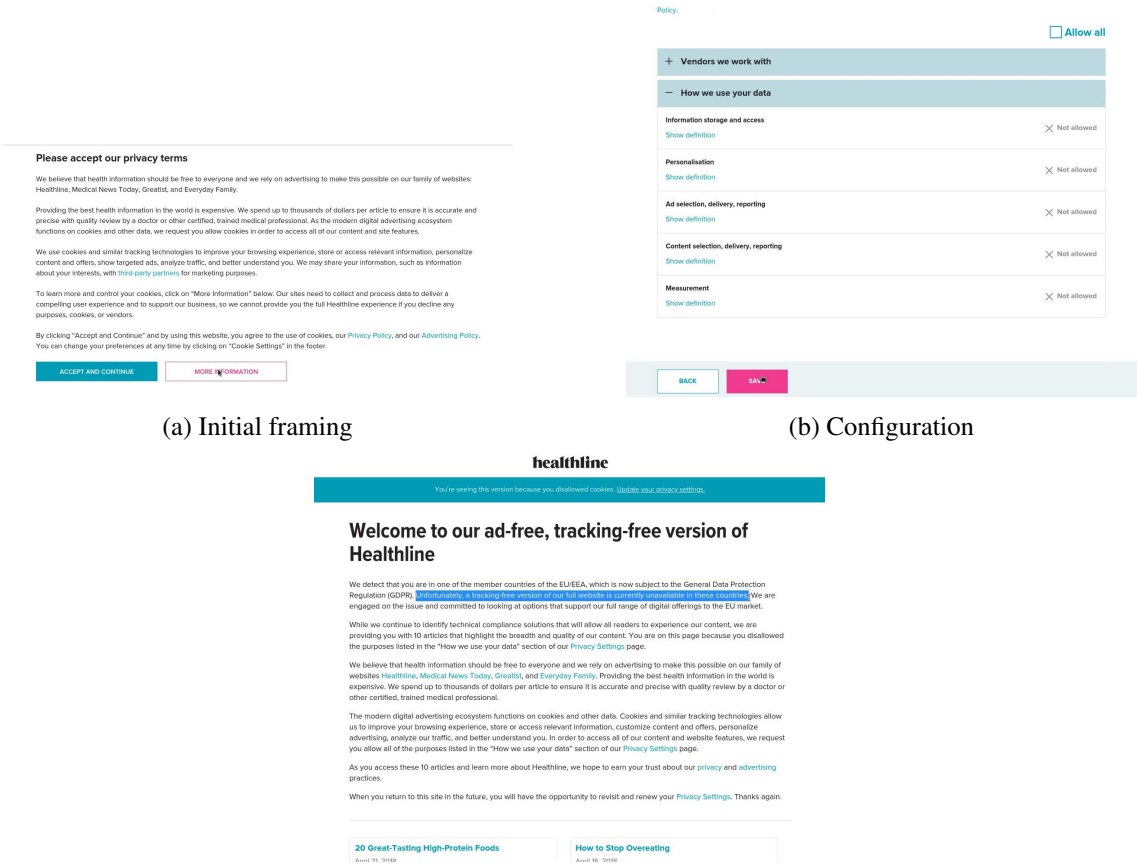
The majority of the stakeholders and regulators concur that failure to consent to the use of trackers should not result in the restriction of access to the website's content. However, the legal prohibition of this practice varies by source, with the European Data Protection Supervisor (EDPS) [75], the European Parliament [76], the Bureau Européen des Unions de Consommateurs (BEUC) [77], the Dutch [78, 79], Belgian [80], German [81], Danish [82] the Greek and Spanish DPAs [83] all agreeing that this practice should be deemed unlawful. In contrast, the ICO [84] and the Austrian [85] DPAs diverge on their opinion of the admissibility of tracking walls. In May 2020, the European Data Protection Board (EDPB) addressed the legitimacy of cookie walls and considered [86, 3.1.2. (39 – 41)] that the requirement for free consent implies that "access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored in the terminal equipment of a user (so called cookie walls)". Thus, using "a script that will block content from being visible except for a request to accept cookies and the information about which cookies are being set and for what purposes data will be processed", with "[. . .] no possibility to access the content without clicking on the 'Accept cookies' button" is regarded as non compliant to the GDPR.

Summary Consistent with our analysis of the consent wall, this design choice increases the tension between interactive separation of user activities and the requirement to allow the user to freely give their consent. In addition to this primary design and legal tension, the lack of an ability to reject consent—alongside the inability to use the web resource without making this forced choice—represents an additional barrier to the user's ability to make a specific and informed decision.

3.4.2 Configuration and Acceptance

3.4.2.1 Reduced Service

The use of *reduced service* refers to the practice of a website offering reduced functionality—for example, allowing a user access to only limited number of pages on a website—based on their consent configuration options. In the scope of this paper, reduced service is a result of the user refusing consent in some or all of the proposed privacy configurations. An extreme case of a reduced service occurs when a website fully blocks access because the user refuses some of the privacy configurations. In one example of this design choice, the website https://www.medicalnewstoday.com/ shows that when the user refuses consent, they are redirected to another website https://anon.healthline.com/, which is a reduced version of the original website with only 10 pre-selected pages available to the user, as depicted in Figure 3.4 §. Interestingly, if the user visits https://www.medicalnewstoday.com/ again after making this configuration choice, the full website is available.



(a) Initial framing

(b) Configuration

(c) Alternate "reduced" version of the website

Figure 3.4 – Example of a reduced service, recorded on 1 October 2019. Credits : healthline.com

§. Video https://mybox.inria.fr/f/1ec82ce1a4dd4f82b556/ recorded on 4 March 2020.

Designer perspective. A reduced service consists of a second version of the website with less functionality, differentiating the content made accessible to the users depending on their acceptance or refusal of all or some of the privacy configuration options. This design decision may reflect the business realities that some designers are forced to consider in relation to stakeholders, such as the role of ad-generated content or other types of tracking that may make publishing certain kinds of content untenable *without* erecting the equivalent of an ineffective paywall. From a *legal perspective*, a reduced service option could be allowed if it clearly enables the user to choose between various options of access. For publishers that provide more means of access (such as free and paid), a reduced service option could be allowed if it clearly lets the user to choose between various options of access. As a boundary condition, the Article 29WP [87] states that refusal of consent must be "without detriment" or "lowering service levels", though such delineation comes without decomposing what this means in concrete settings, particularly in the digital world.

User and interface perspectives. The user, when refusing tracking, is redirected to a different, reduced version of the website, and perhaps without knowledge that they made a choice that impacted the content they received. The ultimate effect here is a degraded experience for these users, a practice which the NCC [88] names *"Reward and punishment"*, explaining that service providers use incentives to reward a correct choice (e.g., extra functionality or a better service), and punish choices they deem undesirable, which in our case entails a refusal of tracking. Thus, the overall effect on the side of the user is either experienced as the dark pattern "forced action" or "obstruction" if the feedforward action upon selection of a consent option clearly results in the user being directed to a site with reduced service, and "interface interference" or "sneaking" if the consent interface does not provide adequate feedforward instructions, or otherwise misrepresents the nature of choice in relation to its impact on the user experience. In this design choice, the specific nature of the interface elements are less important than the destination to which the user is sent, and the extent to which the user interface provides guidance to allow the user to make an informed and freely given choice regarding whether they wish to access a full or reduced version of the site. However, a *freely given consent* implies that the data subject could refuse consent without detriment which could be construed as facing significant negative consequences (Recital 42 of the GDPR).

Moreover, the legal requirement of *informed consent* could be violated under the reduced service design choice. As argued by the General Advocate Szpunar [89], a data subject must be informed of all circumstances surrounding the data processing and its *consequences* : *"crucially, he or she must be informed of the consequences of refusing consent"*, including a reduced service. He proceeds by asserting that *"a customer does not choose in an informed manner if he or she is not aware of the consequences,"* thus potentially rendering instances where feedforward in the interface is missing to be legally problematic. Additionally, this limitation of service, conditional on consent, obliges the user to give consent to the data processing in order to fully access the website, and therefore, in the absence of another access option, may also violate a freely given consent requirement. In a similar line of thought, Acquisti et al. [90] propose that increasing the cost or the difficulty of choosing specific configurations, even at the simple level of requiring multiple confirmations, configures a "punishment" that could prevent inexperienced users from selecting risky settings.

Social impact perspective. From a social impact perspective, we start our analysis by considering the intentions of a website owner, pointing towards broader issues of economic viability.

Reduced service, from one perspective, could be a response to the economic need of the website owner to find a working business model, thus allowing users to access the full version of the website only if they gave a positive consent, and hence the website can be funded indirectly via data collected from the user. Beyond the technical complexity of presenting two or more versions of the same web property, there are also potential issues relating to archival access of content, deep linking, or other forms of user discovery that have become typical in most web experiences. Notions of free and unencumbered access is increasingly problematic on the internet, evidenced by resistance to paying for quality journalism and expectations of access to content through bundling with a larger service (e.g., Netflix, Amazon Prime).

This design choice also points towards potentially relevant legal obligations which are often hidden to end users. The website owner must find a balance between the economic and legal requirements, but the main tool by which they might make this separation may prove to be overly coercive, violating the assumption that consent is "freely given." One way to approach this difficult balance may be to propose users pay for access to the website if consent is refused. However, such paid models lead to further social consequences. A choice between a paid option without tracking and a "free" option, financed by tracking, implies that the user's right to privacy is conditioned to paying a fee, which introduces unequal access to a fundamental right to privacy for different categories of users. This raises the question of the compatibility between (1) the obligation to respect users' rights, equality of rights even when users don't have the same level of income, and (2) the need for funding for the website.

Summary. This design choice presents tensions among separation of access to content based on 1) the consent choice of the user, 2) the economic realities of producing and providing access to content, 3) requirements for consent to be freely given with outcomes that are transparent to the user, and 4) increasing social expectations that web content be accessible without cost or obligation. All these tensions point toward potential acceptance of this design choice, but only in cases where the feedforward interaction—explicitly indicating that certain consent decisions will result in reduced service—is transparent and non-coercive, without the use of sneaking or interface interference dark patterns. However, most instances of this design choice are likely to fail, either by limiting consent choices up front, or by using manipulative language to lull the user into accepting a choice with different consequences than they expect.

3.4.2.2 Other Configuration Barriers

Configuration barriers usually correspond to known implementations of consent mechanisms that dynamically interact with the user and direct them towards acceptance of consent [32, 33]. Configuration choices can be deconstructed into a variety of more basic design choices, such as :

— The imposition of hierarchies or prioritization of choices which should have instead equal value or positioning. We observe this practice in consent dialogs with a larger "OK" button that appears first, and a smaller "Configure" button gives a more prominent visual hierarchy to "OK."

— The introduction of aesthetic manipulation (also known as "attractors" or "interface interference"), where desired and concrete user choices are perceived more salient and prioritized. An example of this phenomenon might include a bright and attractive "accept" button and either a gray "reject" or "more options" button (Figure 3.5).

— The use of reading order manipulation to "sneak" information past the user. One example of this includes the use of a box "I consent" emphasized in a black box, and "More Options" link on the (left) corner of the banner, outside of the normal reading order (Figure 3.6).
— The use of hidden information that is hidden behind another interactive element or otherwise invisible to the user without further investigation. For instance, the use of plain unformatted text to indicate a link to "Preferences," while "Accept" is a visible button.

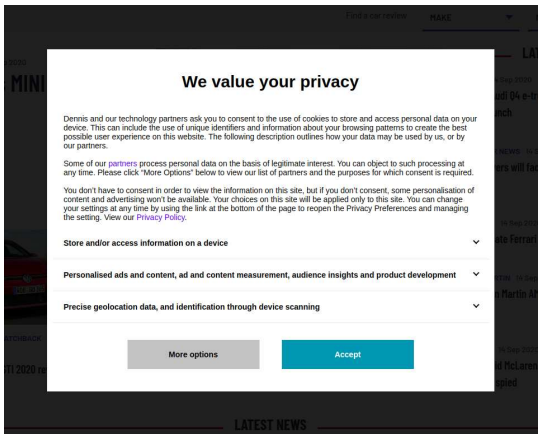


Figure 3.5 – Use of aesthetic manipulation in the presentation of consent options (Credits : autoexpress.co.uk).

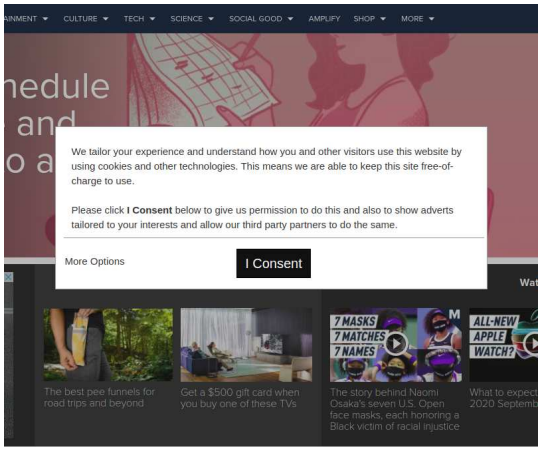


Figure 3.6 – Use of reading order manipulation to discourage certain consent options (Credits : mashable.com).

Below we consider this range of interrelated design choices as a complex set of visual and interactive design criteria (e.g., [91–93]) from which designers can draw in creating design outcomes that allow users to select consent options.

Designer perspective. The designers intent to use influencing factors that are visually salient (e.g., a larger button for "'accept," the use of bright colors for objects with a higher priority, or the use of hovering properties to disguise feedforward) have a clear and direct effect of prioritizing the choice of acceptance of tracking over rejection, even if such choices are less privacy-friendly to the end user. While many of these visual techniques are well known, building upon gestalt psychology principles, and are often used to create more efficient and engaging user experiences, these same principles can be co-opted through the use of "interface interference"-oriented dark patterns.

Interface perspective Specific configuration properties of cookie banners have been manipulated in order to influence users' decision to give consent [43]. The means of manipulation include many aspects of visual and interactive display, including the positioning, size, number of choices given, formatting (use of fonts and colors emphasising consent options, widget inequality), hiding settings behind difficult to see links, preselected boxes, and unlabeled sliders. These *attractors* are interface elements that are intentionally designed to draw or force the attention to a salient portion of a larger interactive experience [94]. The "salient field" is the part of the consent dialog that provides the most important information to aid the user's decision. The use of such eye-catching techniques makes it easier to see and act on some design elements than others, and making some

buttons or options more salient is an example of design outcomes that are intended to surreptitiously nudge users by making a pre-chosen and intended choice more salient [88, pp. 19-20]. From a *legal perspective,* Article 7(4) of the GDPR states that withdrawing consent should be as easy as giving it, and we additionally interpret that the choice between "accept" and "reject" tracking must be consequently balanced and equitable and as such, design choices related to an unbalanced choice violate the legal requirement of an *ambiguous consent*. In fact, "[a] consent mechanism that emphasizes 'agree' or 'allow' over 'reject' or 'block' represents a non-compliant approach, as the online service is influencing users towards the 'accept' option." , [84]. The Advocate General of the Court of Justice of the EU [95] emphasized the need for both actions, "optically in particular, [to] be presented on an equal footing." Thus, while *the procedure to choose should be as simple as to accept* is legally warranted, pointing towards a series of design choices that makes the acceptance and refusal buttons visually balanced (or equitable), the complex array of design choices in play make the practical inclusion or exclusion of certain interface choices difficult to precisely objectify.

User perspective. The apparent need for attractors stems from the fact that *attention is a limited resource* ; consumers are often multi-tasking and focusing on many different stimuli at once [96]. The attentiveness of consumers to privacy issues may be sporadic and limited, inhibiting the usefulness or impact of even simple and clear privacy notices. Therefore the salience of stimuli can impact the user's decision-making processes and outcomes. The configuration practices of *"attention diversion"* [97] draw attention to a point of the website with the intention to distract and/or divert the user from other points that could be useful. The French Data Protection Authority adds that designers can take advantage of user psychology, for instance deciding to make the color of a "continue" button green while leaving the "find out more" or "configure" button smaller or grey. If users are conditioned by the traffic light metaphor bias used by designers that assign colors according to the flow of information ("green" = free flowing ; "red" = stop), users may perceive green as the *preferable choice*.

Social impact perspective. Services offer a carefully designed interface, which rather than configuring a neutral conduit, instead nudge the user into acting in the best interest of the shareholder. While these behavioral techniques are well known in industry settings, most users are not aware of the degree to which their everyday patterns of use are predetermined, based on knowledge of human psychology in general and the actions of users in particular contexts. Many of the visual and interactive choices indicated above are not neutral, but rather—in combination—have been shown through A/B testing or use of other evaluation to produce the desired output behavior from users. Thus, while societal norms at large might dictate that interfaces should not use potentially misleading design practices—such as the use of visual grammar that might lead the user to think that consent is required to continue browsing, or that visually emphasizes the possibility of accepting rather than refusing—the capabilities of digital systems to rapidly test and deploy interface combinations that are optimized for certain behaviors act against our broader desire as a society to make informed and deliberate choices about how our data is collected and used.

Summary These series of overlapping and cascading design choices provide a central point of focus for the desired and actual experience of the consent process. The notion of configuration is central to the ability of the user to make an unambiguous and specific choice about how their

data can be collected and used. However, as shown above, so many of the visual and interactive elements relate and interact in ways that resist the ability of policy to specify allowable and unallowable design choices. While some tactics can be used to provide a better user experience (e.g., use of color to indicate the role of different options and their meaning in relation to feedforward interaction), they can easily be subverted as well. Thus, while the outcomes are clear from a legal perspective, it is virtually impossible to demonstrate in full what design choices are relevant, appropriate, and legal—either separately or in combination.

3.5 Discussion

In the previous sections, we have identified different approaches to engagement with consent banners across the user task flow, including : a) altering the initial framing of the consent experience through a consent wall or tracking wall ; and b) manipulating the configuration and acceptance parameters through reduced service and other barriers to configuration. Using an interaction criticism approach, we described the complex forms of disciplinary engagement and tensions built into each set of design choices as experienced from four different subject positions, including : the designer, the interface itself, the end user, and the broader social impact. In articulating each consent experience from these multiple points of view, we have sought to bring together design, computer science, and legal perspectives, particularly acknowledging instances where these perspectives foreground tensions in satisfying concerns raised from these disciplinary perspectives. Building on our findings—and the many discussions that supported our investigation of consent banners—we present below a further synthesis of our transdisciplinary dialogue. First, we describe how argumentation can be productively commenced and sustained from both design and legal perspectives. Second, we build upon this mode of argumentation to describe new opportunities for dialogue across legal, ethics, computer science, and HCI perspectives to engage with matters of ethical concern through the lens of dark patterns.

3.5.1 Bi-directional Design and Legal Argumentation

We have demonstrated the value of approaching a complex issue such as the design and regulation of consent experiences from the perspective of multiple disciplines, revealing through our analysis a range of synergies and disconnects between these perspectives. We argue that although there is a desire for standardization, enabling the exercise of a valid choice by end-users, there does not appear to be a fully neutral set of design requirements by which operators can guarantee that all elements of the GDPR can be satisfied. When engaging in a bi-directional means of argumentation between design and legal perspectives, we can identify some of the areas of tension and opportunity—pointing to new possibilities for policy implementation, and better ways of managing legal requirements during the design and development process. By “bi-directional,” we refer to the opportunities to evaluate and interrogate designed experiences using the language of law and policy (legal->design), while also using a user experience or user interface as a means of addressing gaps or opportunities for more precision in existing legal or policy frameworks (design->legal).

Beginning from a legal perspective, we can envision the role of standardization in consenting procedures, including a list of ambiguous behaviors that must be explicitly acknowledged by decision-makers. Ensuring standardization could enable rapid detection of violations at scale

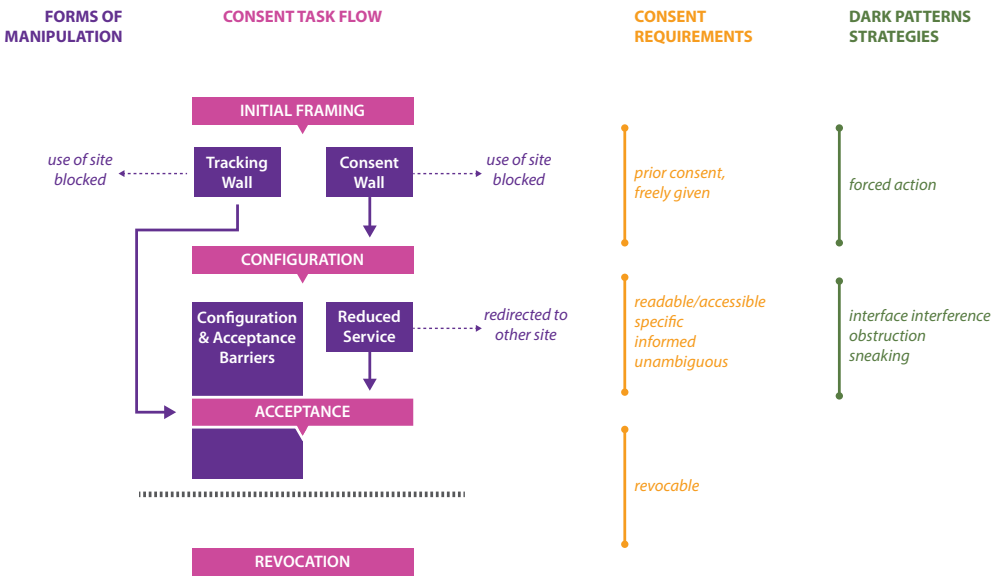


Figure 3.7 – Flowchart describing the forms of manipulation we observed in our dataset in relation to the consent task flow, legal consent requirements, and dark patterns strategies.

(building on similar work in e-commerce by Mathur et al. [29]) while also minimizing legal uncertainty and subject appraisal regarding configuration aspects of consent banners. Using a standardization approach could also minimize behaviors presenting a margin of doubt regarding the choice expressed by the user, as advocated in recent work [40, 98]. When interrogating this desire for standardization from a design perspective, we can see deficiencies in the current data protection framework which do not accurately model or describe relevant HCI, UI, and UX elements when assessing the lawfulness of dark patterns in consent formulation. While previous empirical work acknowledges the impact that HCI and UI provokes in the user's decision-making process (e.g., [32, 33, 35]), it is currently unclear whether fully "neutral" design patterns exist, and even if they did, how a list of possible misleading design practices that impact both users' perception and interaction that impact a compliant consent could be fully dictated *a priori*.

Using Figure 3.7 as a guide, we can begin to identify legal and design/HCI/UX endpoints with which to start a conversation, revealing various disciplinary perspectives that have the potential to guide future policy and design decisions. It is clear that even if some of these disciplinary perspectives may appear debatable or blurred when presented through the practice of interaction criticism, the disconnects and synergies signifies instead a space of vitality and opportunity at the nexus of these domains that may point towards patterns that *should* be illegal and patterns that are more *likely* to produce a fully-compliant consent. We propose that developments will be more rapidly identified and consolidated when the transdisciplinary perspectives across legal, ethics and HCI scholarship are integrated within case-law and also validated in academic research. In particular, a reading of this figure allows researchers, designers, and legal scholars to identify spaces where social and political values might successfully emerge together or collide, recognizing that the foregrounding of certain perspectives and language indicates that ethical engagement with these issues is always already political and value-laden. The political and ethical dimensions of

design choices requires designers, researchers, and legal scholars alike to use a pragmatist ethics approach to identify and rationalize design choices in relation to legal requirements, user value, and potential or actual societal impact.

3.5.2 Opportunities to Bridge Legal, Ethics, and HCI Scholarship

Building on the need for bi-directional argumentation shown above, we see a opportunity for further interwovenness between design choices and legal guidance, using this liminal space as a means of describing ways to engage in more transdisciplinary ways underneath the conceptual umbrella of "dark patterns." While other conceptual means of connecting these disciplinary perspectives are possible and potentially useful, we will that demonstrate the conceptual unity among these perspectives—bringing together scholars from many disciplinary perspectives— is possible in the sections delved below.

First, while assessing each consent experience, we observed a *tension* between dark pattern categories because many dark patterns overlap in the different visual and interactive design choices of a single banner [33]. These patterns are blurred and difficult to distinguish, and in fact, we as human evaluators frequently disagreed on which dark pattern might exist on a specific banner, and from which perspective one evaluation may be more or less tractable. For example, obstruction and interface interference are often perceived at the same time, but are perhaps co-constitutive; interface interference foregrounds a visual design and gestalt psychology perspective, while obstruction foregrounds a view of the temporal user journey and user goals. This difference in perspective reveals that any analysis on design choices and the detection of dark patterns is *interpretive* and therefore there is need for different and combined methods. Though some dark patterns have been successfully detected through computational means [29], many of the aspects of user experience that we highlighted above cannot be easily detected automatically, and may be revealed only through a manual analysis and consideration of multiple user and interactive characteristics. **This insight reveals that dark patterns is a n-dimensional phenomenon which includes dimensions of time, interaction, design, psychology, and law—demanding a holistic analysis from many perspectives.**

Second, we have revealed that some of the analyzed design choices correspond to known classifications of dark patterns and moreover, they fit neatly within current regulatory structures that prohibit and sanction deceptive practices, as it is the case of tracking walls, which are explicitly forbidden by the European Data Protection Board [86]. Thus, these design choices should be considered legally actionable and subject to enforcement actions by the competent authorities. Conversely, some design choices might be deemed as unlawful, but fail to fit the threshold of what is mandated by explicit legal requirements, though arguably falling outside of existing data protection regimes (for example, the case of reduced service). Regarding the role of design choices that might trigger legal or policy implications, we agree with Schaub et al. [99] and Karegar et al. [100] which argue that the main problem might not be inherent to the requirements postulated by current legal sources, but in how consent dialogs are currently designed. This disjuncture in potential outcomes points to two plausible directions for bridging and transdisciplinary discourse : a) a pathway towards recognition of design choices that are knowingly applied by designers that are demonstrably causal in producing impact that is negative from a user or legal perspective, and are unnecessarily disruptive in a way that could be deemed unlawful ; and b) a means of identifying and encouraging discourse among everyday users around practices which are not unlawful *per se*, but which should nevertheless be discouraged.

In the first case, active empirical work is needed to determine causality in conjunction with identification of other important variables that must be considered to eventually determine the lawfulness of the relevant design choice(s). Therefore, while the current legal regulatory scope regarding dark patterns in these cases might not be sufficient, it could be established through both empirical and practical means. The use of stricter regulations for consent banners that prohibit and sanction evidence-based misleading design practices might not be sufficient on their own to reestablish a privacy-friendly environment. Recent experimental work [35] has shown that even after removing a nudging and manipulative design choice, a form of routinised conditioning could still *persist*, ultimately leading users to behave in a certain way, due to an irreflective default behavior, referred as "effect survival" by Hertwig and Grune-Yanoff [101]. Notwithstanding, the incoming ePrivacy Regulation [76] might install a "Do not Track" mechanism that would be mandatory for all sites, limiting the number of times users are asked to consent to tracking.

In the second case, broader public and professional participation may be needed to identify negative practices, facilitating users to "name and shame" companies that use these patterns and professionals to identify such patterns as irresponsible or destructive within codes of ethics or other constraining professional criteria, as originally proposed by Brignull in relation to dark patterns [59]. Such developments reflect the point that designers are increasingly required to respond with ethically-valenced decisions beyond what may be strictly provided for within legal frameworks and that these design decisions are not neutral, but rather reveal the assignment of value and power. **More transdisciplinary collaborative research and engagement is needed to translate such abstract debates into practical policy or professional outcomes and to prevent any potential "moral overload" in relation to the difficult decisions requiring complicated trade-offs and reflection.**

Third, we have shown that illegal and unlabeled dark patterns can emerge from new analysis, building on the work of Soe et al. [33] and Matte et al [34] and our own application of interaction criticism. For example, the design choices "consent wall" and "reduced service"—while relying upon the dark patterns of obstruction and forced action—are not included in pre-existing categorizations of dark patterns, as defined by others [24, 25, 29, 43, 46, 97], but rather they emerged from a discussion between legal experts, designers, and computer scientists who are the authors of this paper. We find it likely that there may be many other types of dark patterns that can be revealed when users interact with consent banners, along with many other means of engaging with data privacy and security. In contrast to this discovery of the "darkness" of user interactions, we also present the opportunity to identify new ways to empower users through "bright" or "light" patterns [101], even though empirical research has rendered such pro-privacy nudging approaches as implausible for companies to implement since they are incentivized by tracking user's online behavior. One path towards patterns that result in empowerment, supporting the notion of data protection by default and by design (Article 25 of the GDPR), could be accomplished by making the user's decision to share personal information more meaningful—a technique that Stark [102] refers to as "'data visceralization'—making the tie between our feelings and our data visible, tangible, and emotionally appreciable." In this latter case, **we point towards the potential role for HCI, UI, and UX designers to work in concert with computer scientists and data privacy experts to further reflect the needs of users into technology design to respond to the regulatory challenges in a more contextually aware manner.**

Fourth, we have raised the question of whether the end-user should solely be considered a central to the decision-making process, and if it is a defensible choice to create this burden and expect a reasoned and fully-informed choice *only* from the user. We posit that the GDPR places

substantial—and perhaps unwarranted—pressure on the user by defining the act of consent as a legal basis for processing personal data via tracking technologies. The definition of consent itself places the burden of choice on the user (through unambiguously given consent) and therefore pressure on the user as well. Such weight comes in the form of a design of the consent interface that a user faces when browsing the internet on a daily basis, and in the long term ramifications of the consent choice, which are never fully knowable. Such an assessment happens in often complex decision-making *contexts* where information is processed quickly, choices abound, and cognitive effort is demanded for the user, making this space a prime opportunity for companies to include dark patterns to encourage certain choices and discourage others [103]. Some user-centered approaches to ameliorate the problems found in the current consent system have been studied, such as the use of "bright patterns" and "educative nudges" in combination [35]. *"Bright patterns"* (also known as "non-educative nudges") have been used to successfully nudge users towards privacy-friendly options, but these approaches lead to similar problems as their dark counterparts, namely an unreflective default behaviour and users' general perception of a lack of control. The use of *"educative nudges"* could also be used as reminders or warnings, providing feedback about possible consequences of a user's choice when consenting, however, as the majority of the companies have incentives to track users—nudging them through privacy-unfriendly options—the practical feasibility of such nudges is questionable. Given our experience in working in the legal, computer science, and design fields, we have observed how design choice architectures relying on dark patterns can influence user consent agreements on the data collection and usage in web tracking and that such design choices raise important legal consequences. We raise the question if potentially there are other ways to make a choice that does not rely on solely on consent as it is currently understood, but on another legal basis, deviating some or all the attention from the end-user. **The deeper we look at consent mechanisms and the matter of user choice, the more we understand the need to combine the perspectives of different fields (e.g., HCI, design, UX, psychology, law) as part of a transdisciplinary dialogue in order to ensure that the user's choice indeed satisfies all the consent requirements to be deemed valid : free, informed, specific, unambiguous, readable and accessible.**

3.6 Implications and Future Work

This analysis points towards multiple productive areas for further investigation of the intersections and synergies of legal, ethics, and HCI perspectives on privacy. First, we propose new connections among policymakers and HCI scholarship, building on the work of Spaa et al. [68] in identifying ways "to harness the more speculative and co-productive modes of knowledge generation that are been innovated on by HCI researchers to become part of governmental policymaking processes." This effort could be supported by attending in more detail to the ways in which ethical concerns are languaged, with new scholarship mapping opportunities to connect design concepts, notions of design intent, and opportunities for policy to be crafted. Second, the interaction criticism approach we have taken in this paper highlights the value of thinking and interacting with design artifacts across multiple disciplinary perspectives, including transdisciplinary means of thinking through, verbalizing, and conceptualizing design evidence and argumentation. This means of criticism connects with broader goals for design and HCI education and research, including the need for individuals in a transdiscipline such as HCI to be able to raise, respond to, and encourage discourse around multiple disciplinary perspectives. While we cannot claim our application of

interaction criticism relating to consent concerns as a distinct methodology for transdisciplinary research engagement from this study only, but we have identified specific aspects of disciplinarity and conceptual vocabulary through the use of interaction criticism—both in terms of productive tensions and means of working out aspects of complexity—that have proven to be useful in building a shared language among our varying disciplinary backgrounds that may be helpful in supporting future transdisciplinary work. More research that focuses on the pathways to building competence in this transdisciplinary dialogue—including the ability to raise both synergies among disciplinary perspectives, and also identify disconnects between language, outcomes, and means of argumentation—could productively reveal best practices for educating the next generation of HCI and UX designers and researchers. Third, perhaps the strongest space for further work is in the integration of legal argumentation in design work, as a means of guiding design practices and as a way of extending and productively complicating legal and policy work. The use of speculative modes of argumentation and interrogation of design artifacts, as proposed by Spaa et al. [68], could lead to the creation of better policies that account for potential futures rather than only deterring known practices. This is an opportunity both to extend the purview of design work, as well as a way of better connecting epistemologies of design and law together in ways that lead to positive societal impact.

3.7 Conclusion

In this paper, we present an analysis of consent banners through the *interaction criticism* approach, with the goal of bringing together the language and conceptual landscape of HCI, design, privacy and data protection, and legal research communities. Through our analysis, we have demonstrated the potential for synergies and barriers among these perspectives that complicate the act of designing consent banners. Using the language of dark patterns, we have shown the potential for argumentation across legal and design perspectives that point towards the limitations of policy and the need to engage more fully with multiple perspectives of argumentation. Building on our analysis, we identify new ways in which HCI, design, and legal scholarship and discourse may be productively combined with the goal of translating matters of ethical concern into durable and effective public policy.

3.8 Acknowledgement

This work is funded in part by the National Science Foundation under Grant No. 1909714, ANR JCJC project PrivaWeb (ANR-18-CE39-0008), and by the Inria DATA4US Exploratory Action project.

Bibliography

[1] R. E. Anderson, D. G. Johnson, D. Gotterbarn, and J. Perrolle, "Using the new ACM code of ethics in decision making," *Communications of the ACM*, vol. 36, no. 2, pp. 98–107, 1993. [Online]. Available : http://doi.acm.org/10.1145/151220.151231

[2] D. Gotterbarn, "Reconstructing the ACM code of ethics and teaching computer ethics," *ACM SIGCSE Bulletin*, vol. 30, no. 4, pp. 9–11, 1998. [Online]. Available : https://dl.acm.org/citation.cfm?doid=306286.306293

[3] M. J. Wolf, "The ACM code of ethics : a call to action," *Communications of the ACM*, vol. 59, no. 12, pp. 6–6, 2016. [Online]. Available : https://dl.acm.org/citation.cfm?doid=3022085.3012934

[4] D. Gotterbarn, A. Bruckman, C. Flick, K. Miller, and M. J. Wolf, "ACM code of ethics : a guide for positive action," *Communications of the ACM*, vol. 61, no. 1, pp. 121–128, 2017. [Online]. Available : https://dl.acm.org/citation.cfm?doid=3176926.3173016

[5] A. McNamara, J. Smith, and E. Murphy-Hill, "Does ACM's code of ethics change ethical decision making in software development ?" in *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ser. ESEC/FSE 2018. Association for Computing Machinery, 2018, pp. 729–733. [Online]. Available : https://doi.org/10.1145/3236024.3264833

[6] C. Detweiler, A. Pommeranz, and L. Stark, "Methods to account for values in human-centered computing," in *Proceedings of the 2012 ACM annual conference extended abstracts on Human Factors in Computing Systems Extended Abstracts - CHI EA '12*. ACM Press, 2012, p. 2735. [Online]. Available : http://dl.acm.org/citation.cfm?doid=2212776.2212708

[7] B. Friedman and D. G. Hendry, *Value Sensitive Design : Shaping Technology with Moral Imagination*. MIT Press, 2019. [Online]. Available : https://market.android.com/details?id=book-C4FruwEACAAJ

[8] K. Shilton, "Values and ethics in Human-Computer interaction," *Foundations and Trends® Human–Computer Interaction*, vol. 12, no. 2, pp. 107–171, 2018. [Online]. Available : http://dx.doi.org/10.1561/1100000073

[9] L. Bannon, J. Bardzell, and S. Bødker, "Reimagining participatory design," *Interactions*, vol. 26, no. 1, pp. 26–32, 2018. [Online]. Available : https://dl.acm.org/citation.cfm?doid=3301428.3292015

[10] P. Olivier and P. Wright, "Digital civics : taking a local turn," *Interactions*, vol. 22, no. 4, pp. 61–63, 2015. [Online]. Available : http://dl.acm.org/ft_gateway.cfm?id=2776885&type=html

[11] C. DiSalvo, J. Lukens, T. Lodato, T. Jenkins, and T. Kim, "Making public things : how HCI design can express matters of concern," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, 2014, pp. 2397–2406. [Online]. Available : http://dl.acm.org/citation.cfm?doid=2556288.2557359

[12] ACM U.S. Technology Policy Committee, "Statement on principles and prerequisites for the development, evaluation and use of unbiased facial recognition technologies," Association for Computing Machinery, techreport, 2020. [Online]. Available : https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf

[13] S. M. West, "Data capitalism : Redefining the logics of surveillance and privacy," *Business & Society*, vol. 58, no. 1, pp. 20–41, 2019. [Online]. Available : https://doi.org/10.1177/0007650317718185

[14] R. N. Zaeem and K. S. Barber, "The effect of the GDPR on privacy policies : Recent progress and future promise," *ACM Transactions on Management of Information Systems*, vol. 0, no. ja, 2020. [Online]. Available : https://doi.org/10.1145/3389685

[15] S. Frenkel, M. Isaac, C. Kang, and G. J. X. Dance, "Facebook employees stage virtual walkout to protest trump posts," 2020. [Online]. Available : https://www.nytimes.com/2020/06/01/technology/facebook-employee-protest-trump.html

[16] P. Suciu, "Brands aren't social distancing from social media, they're boycotting !" 2020. [Online]. Available : https://www.forbes.com/sites/petersuciu/2020/07/01/brands-arent-social-distancing-from-social-media-theyre-boycotting/

[17] "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, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[18] "California consumer privacy act of 2018 [1798.100 - 1798.199] (ccpa)," 2018, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[19] C. M. Gray and S. S. Chivukula, "Ethical mediation in UX practice," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. ACM Press, 2019, p. 178. [Online]. Available : http://dx.doi.org/10.1145/3290605.3300408

[20] R. Kirkham, "Using european human rights jurisprudence for incorporating values into design," in *DIS'20 : Proceedings of the Designing Interactive Systems Conference 2020*. ACM, 2020, pp. 115–128. [Online]. Available : https://dx.doi.org/10.1145/3357236.3395539

[21] K. Shilton, "Values Levers : Building Ethics into Design," *Science, technology & human values*, vol. 38, no. 3, pp. 374–397, 2013. [Online]. Available : https://doi.org/10.1177/0162243912436985

[22] K. Shilton and S. Anderson, "Blended, not bossy : Ethics roles, responsibilities and expertise in design," *Interacting with computers*, vol. 29, no. 1, pp. 71–79, 2017. [Online]. Available : https://academic.oup.com/iwc/article-lookup/doi/10.1093/iwc/iww002

[23] M. Steen, "Upon opening the black box and finding it full : Exploring the ethics in design practices," *Science, technology & human values*, vol. 40, no. 3, pp. 389–420, 2015. [Online]. Available : https://doi.org/10.1177/0162243914547645

[24] H. Brignull, "Dark patterns : inside the interfaces designed to trick you," http://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you, 2013. [Online]. Available : http://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you

[25] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The Dark (Patterns) Side of UX Design," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. dl.acm.org, 2018, pp. 534 :1–534 :14. [Online]. Available : https://doi.acm.org/10.1145/3173574.3174108

[26] C. M. Gray, S. S. Chivukula, and A. Lee, "What kind of work do "asshole designers" create ? describing properties of ethical concern on reddit," in *DIS'20 : Proceedings of the Designing Interactive Systems Conference 2020*, ser. DIS'20. ACM Press, 2020, pp. 61–73. [Online]. Available : https://dx.doi.org/10.1145/3357236.3395486

[27] S. Greenberg, S. Boring, J. Vermeulen, and J. Dostal, "Dark patterns in proxemic interactions : A critical perspective," in *Proceedings of the 2014 Conference on Designing Interactive Systems*, ser. DIS '14. ACM, 2014, pp. 523–532. [Online]. Available : http://doi.acm.org/10.1145/2598510.2598541

[28] A. Mirnig and M. Tscheligi, "(don't) join the dark side : An initial analysis and classification of regular, anti-, and dark patterns," in *PATTERNS 2017 : Proceedings of the 9th International Conference on Pervasive Patterns and Applications*, 2017, pp. 65–71. [Online]. Available : https://uni-salzburg.elsevierpure.com/en/publications/dont-join-the-dark-side-an-initial-analysis-and-classification-of

[29] A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan, "Dark patterns at scale : Findings from a crawl of 11K shopping websites," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, p. Article No. 81, 2019. [Online]. Available : https://dl.acm.org/citation.cfm?doid=3371885.3359183

[30] A. Narayanan, A. Mathur, M. Chetty, and M. Kshirsagar, "Dark patterns : Past, present, and future : The evolution of tricky user interfaces," *ACM Queue*, vol. 18, no. 2, p. 67–92, Apr. 2020. [Online]. Available : https://doi.org/10.1145/3400899.3400901

[31] "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance). Directive 2009/136/EC," 2009, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136.

[32] 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*, ser. CHI '20. Association for Computing Machinery, 2020, pp. 1–13. [Online]. Available : https://doi.org/10.1145/3313831.3376321

[33] T. H. Soe, O. E. Nordberg, F. Guribye, and M. Slavkovik, "Circumvention by design-dark patterns in cookie consent for online news outlets," *NordiCHI '20 : Proceedings of the 11th Nordic Conference on Human-Computer Interaction : Shaping Experiences, Shaping Society*, 2020.

[34] C. Matte, C. Santos, and N. Bielova, "Do cookie banners respect my choice ? measuring legal compliance of banners from iab europe's transparency and consent framework," in

IEEE Symposium on Security and Privacy (IEEE S&P 2020). Accepted for publication. IEEE, 2020, pp. 791–809.

[35] P. Grassl, H. Schraffenberger, F. Zuiderveen Borgesius, and M. Buijzen, "Dark and bright patterns in cookie consent requests," 2020. [Online]. Available : psyarxiv.com/gqs5h

[36] J. Bardzell, "Interaction criticism : An introduction to the practice," *Interacting with computers*, vol. 23, no. 6, pp. 604–621, 2011. [Online]. Available : http://dx.doi.org/10.1016/j.intcom.2011.07.001

[37] R. E. Leenes and E. Kosta, "Taming the cookie monster with dutch law - a tale of regulatory failure," *Computer Law & Security Review*, vol. 31, pp. 317–335, 2015.

[38] R. E. Leenes, "The cookiewars : From regulatory failure to user empowerment ?" in *The Privacy & Identity Lab*. The Privacy & Identity Lab, 2015, pp. 31–49.

[39] E. Kosta, "Peeking into the cookie jar : the european approach towards the regulation of cookies," *I. J. Law and Information Technology*, vol. 21, pp. 380–406, 2013.

[40] C. Santos, N. Bielova, and C. Matte, "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*, pp. 91–135, 2020. [Online]. Available : https://doi.org/10.26116/techreg.2020.009

[41] J. B. Luguri and L. J. Strahilevitz, "Shining a light on dark patterns," 2019, public Law Working Paper No. 719. [Online]. Available : https://ssrn.com/abstract=3431205

[42] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems : A user study of consent dialogs after GDPR," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 481–498, 2020. [Online]. Available : https://content.sciendo.com/view/journals/popets/2020/2/article-p481.xml

[43] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(un)informed consent : Studying GDPR consent notices in the field," in *Conference on Computer and Communications Security*. ACM, 2019, pp. 973–990.

[44] S. Human and F. Cech, "A Human-Centric perspective on digital consenting : The case of GAFAM : Proceedings of KES-HCIS 2020 conference," in *Human Centred Intelligent Systems*, ser. Smart Innovation, Systems and Technologies, A. Zimmermann, R. J. Howlett, and L. C. Jain, Eds. Springer Singapore, 2021, vol. 189, pp. 139–159. [Online]. Available : https://link.springer.com/10.1007/978-981-15-5784-2_12

[45] B. Friedman, P. Kahn, and A. Borning, "Value sensitive design : Theory and methods," University of Washington Dept. Of Computer Science & Engineering, Tech. Rep., 2002. [Online]. Available : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.8020&rep=rep1&type=pdf

[46] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "Tales from the dark side : Privacy dark strategies and privacy dark patterns," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 4, pp. 237–254, 2016. [Online]. Available : https://www.degruyter.com/view/j/popets.2016.2016.issue-4/popets-2016-0038/popets-2016-0038.xml

[47] S. S. Chivukula, C. Watkins, R. Manocha, J. Chen, and C. M. Gray, "Dimensions of UX practice that shape ethical awareness," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI'20. ACM Press, 2020, pp. 1–13. [Online]. Available : http://dx.doi.org/10.1145/3313831.3376459

[48] C. R. Watkins, C. M. Gray, A. L. Toombs, and P. Parsons, "Tensions in enacting a design philosophy in UX practice," in *DIS'20 : Proceedings of the Designing Interactive Systems Conference 2020*, ser. DIS'20. ACM Press, 2020, pp. 2107–2118. [Online]. Available : http://dx.doi.org/10.1145/3357236.3395505

[49] K. Shilton, "Engaging values despite neutrality : Challenges and approaches to values reflection during the design of internet infrastructure," *Science, technology & human values*, vol. 43, no. 2, p. 016224391771486, 2018. [Online]. Available : https://doi.org/10.1177/0162243917714869

[50] K. Shilton, J. A. Koepfler, and K. R. Fleischmann, "How to see values in social computing : methods for studying values dimensions," in *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing - CSCW '14*. ACM Press, 2014, pp. 426–435. [Online]. Available : http://dl.acm.org/citation.cfm?doid=2531602.2531625

[51] M. L. Cummings, "Integrating ethics in design through the value-sensitive design approach," *Science and engineering ethics*, vol. 12, no. 4, pp. 701–715, 2006. [Online]. Available : https://www.ncbi.nlm.nih.gov/pubmed/17199145

[52] A. van Wynsberghe, "Designing robots for care : care centered value-sensitive design," *Science and engineering ethics*, vol. 19, no. 2, pp. 407–433, 2013. [Online]. Available : http://dx.doi.org/10.1007/s11948-011-9343-6

[53] A. Borning and M. Muller, "Next steps for value sensitive design," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012, pp. 1125–1134. [Online]. Available : http://dl.acm.org/citation.cfm?doid=2207676.2208560

[54] N. Manders-Huits, "What values in design ? the challenge of incorporating moral values into design," *Science and engineering ethics*, vol. 17, no. 2, pp. 271–287, 2011. [Online]. Available : http://dx.doi.org/10.1007/s11948-010-9198-2

[55] J. Davis and L. P. Nathan, "Value sensitive design : Applications, adaptations, and critiques," in *Handbook of Ethics, Values, and Technological Design : Sources, Theory, Values and Application Domains*, J. van den Hoven, P. E. Vermaas, and I. van de Poel, Eds. Springer Netherlands, 2021, pp. 1–26. [Online]. Available : https://doi.org/10.1007/978-94-007-6994-6_3-1

[56] N. Jacobs and A. Huldtgren, "Why value sensitive design needs ethical commitments," *Ethics and information technology*, pp. 0–0, 2018. [Online]. Available : https://doi.org/10.1007/s10676-018-9467-3

[57] C. A. Le Dantec, E. S. Poole, and S. P. Wyche, "Values as lived experience : evolving value sensitive design in support of value discovery," in *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM Press, 2009, pp. 1141–1150. [Online]. Available : http://dx.doi.org/10.1145/1518701.1518875

[58] C. Nodder, *Evil by Design : Interaction Design to Lead Us into Temptation*. John Wiley & Sons, Inc., 2013. [Online]. Available : https://market.android.com/details?id=book-46Wl1G9yJUoC

[59] H. Brignull, M. Miquel, J. Rosenberg, and J. Offer, "Dark patterns - user interfaces designed to trick people," http://darkpatterns.org/, 2015. [Online]. Available : http://darkpatterns.org/

[60] J. Hoepman, "Privacy design strategies," *Privacy Law Scholars Conference (PLSC)*, vol. abs/1210.6621, 2013.

[61] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "," 2016, https://dark.privacypatterns.eu/.

[62] M. Maier and R. Harr, "Dark design patterns : An End-User perspective," *Human Technology*, vol. 16, no. 2, pp. 170–199, 2020. [Online]. Available : http://dx.doi.org/10.17011/ht/urn.202008245641

[63] C. M. Gray, J. Chen, S. S. Chivukula, and L. Qu, "End user accounts of dark patterns as felt manipulation," Oct. 2020.

[64] L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba, and A. Bacchelli, "UI dark patterns and where to find them : A study on mobile applications and user perception," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI '20. New York, NY, USA : Association for Computing Machinery, Apr. 2020, pp. 1–14. [Online]. Available : https://doi.org/10.1145/3313831.3376600

[65] A. E. Waldman, "There is no privacy paradox : How cognitive biases and design dark patterns affect online disclosure," 2019. [Online]. Available : https://www.sciencedirect.com/science/article/pii/S2352250X19301484

[66] M. Dieter, "Dark patterns : Interface design, augmentation and crisis," in *Postdigital Aesthetics : Art, Computation and Design*, D. M. Berry and M. Dieter, Eds. Palgrave Macmillan UK, 2015, pp. 163–178. [Online]. Available : https://doi.org/10.1057/9781137437204_13

[67] S. S. Chivukula, C. Watkins, L. McKay, and C. M. Gray, ""nothing comes before profit" : Asshole design in the wild," in *CHI EA '19 : CHI'19 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2019, p. LBW1314. [Online]. Available : http://dx.doi.org/10.1145/3290607.3312863

[68] A. Spaa, A. Durrant, C. Elsden, and J. Vines, "Understanding the boundaries between policymaking and HCI," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York, NY : ACM Press, 2019. [Online]. Available : http://dx.doi.org/10.1145/3290605.3300314

[69] "Judgment in case c-673/17 bundesverband der verbraucherzentralen und verbraucherverbände – verbraucherzentrale bundesverband ev v planet49 gmbh," 2019, http://curia.europa.eu/juris/documents.jsf?num=C-673/17.

[70] M. Q. Patton, *Qualitative evaluation and research methods*, 3rd ed. Thousand Oaks : Sage Publications, 2001.

[71] IAB Europe, "IAB europe transparency & consent framework policies (v. 1.1)," Tech. Rep., 2019. [Online]. Available : https://iabeurope.eu/wp-content/uploads/2019/08/IABEurope_TransparencyConsentFramework_v1-1_policy_FINAL.pdf

[72] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco : A Research-Oriented top sites ranking hardened against manipulation," Jun. 2018. [Online]. Available : http://arxiv.org/abs/1806.01156

[73] F. Borgesius, S. Kruikemeier, S. Boerman, and N. Helberger, "Tracking walls, take-it-or-leave-it choices, the gdpr, and the eprivacy regulation," *European Data Protection Law Review*, vol. 3, pp. 353–368, 2017.

[74] C. N. I. et Libertés (CNIL), "On the practical procedures for collecting the consent provided for in article 82 of the french data protection act, concerning operations of storing or gaining

access to information in the terminal equipment of a user (recommendation "cookies and other trackers"),," https://www.cnil.fr/sites/default/files/atoms/files/draft_recommendation_cookies_and_other_trackers_en.pdf.

[75] EDPS, "EDPS opinion 6/2017 on the proposal for a regulation on privacy and electronic communications (ePrivacy Regulation)," 2017.

[76] European Parliament, "Report on the 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),(COM(2017)0010 – C8-0009/2017 – 2017/0003(COD))," 2019, https://www.parlament.gv.at/PAKT/EU/XXVII/EU/01/51/EU_15125/imfname_10966469.pdf.

[77] BEUC, "Position Paper, 'Proposal For A Regulation On Privacy And Electronic Communications (E-Privacy)'," 2019, www.beuc.eu/publications/beuc-x-2017-059_proposal_for_a_regulation_on_privacy_and_electronic_communications_e-privacy.pdf.

[78] Autoriteit Persoonsgegevens, "Cookies," 2019, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#mag-ik-als-organisatie-een-cookiewall-gebruiken-7111.

[79] House of Representatives of the Netherlands, "Answer to questions from members Middendorp and Van Gent about a possible cookie wall ban," 2019, www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2019D49667&did=2019D49667.

[80] Belgian DPA, "Cookies," 2019, www.autoriteprotectiondonnees.be/faq-themas/cookies.

[81] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI, German DPA), "Guidance from german authorities for telemedia providers (translation)," https://deutschland.taylorwessing.com/de/documents/get/1820/guidance-from-german-authorities-for-telemedia-providers-partial-translation.PDF_show_on_screen, accessed on 2020.01.21.

[82] Datatilsynet, "Guide on consent," 2019, www.datatilsynet.dk/media/6562/samtykke.pdf.

[83] Agencia Española de Protección de Datos(AEPD), "Guide on the use of cookies," 2019, www.aepd.es/media/guias/guia-cookies.pdf.

[84] I. C. Office, "Guidance on the use of cookies and similar technologies," 2019, https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf.

[85] Österreichische Datenschutzbehörde, "Decision on the validity of consent," 2018, www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.pdf.

[86] European Data Protection Board (EDPB), "Guidelines 05/2020 on consent under regulation 2016/679," 2020. [Online]. Available : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[87] Article 29 Working Party, "Guidelines on consent under Regulation 2016/679" (WP259 rev.01), adopted on 10 April 2018," 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[88] Frobrukerrådet (Norwegian Consumer Council), "Deceived by design : How tech companies use dark patterns to discourage us from exercising our rights to privacy," 2018. [Online]. Available : https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design

[89] Opinion of Advocate General Szpunar, "Opinion of the Case C-61/19 Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)," 2020, eCLI :EU :C :2020 :158 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62019CC0061.

[90] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. M. Sadeh, F. Schaub, M. Sleeper, Y. Wang, and S. Wilson, "Nudges for privacy and security : Understanding and assisting users' choices online," *ACM Comput. Surv.*, vol. 50, pp. 44 :1–44 :41, 2017.

[91] D. Benyon, *Designing interactive systems : a comprehensive guide to HCI and interaction design*. Harlow, UK : Pearson Education Limited, Jan. 2014.

[92] A. Cooper, R. Reimann, D. Cronin, and C. Noessel, *About face : the essentials of interaction design*. Indianapolis, IN : John Wiley & Sons, Jan. 2014.

[93] J. Tidwell, *Designing Interfaces : Patterns for Effective Interaction Design*. O'Reilly Media, Inc., Dec. 2010. [Online]. Available : https://market.android.com/details?id=book-5gvOU9X0fu0C

[94] C. Bravo-Lillo, L. F. Cranor, S. Komanduri, S. E. Schechter, and M. Sleeper, "Harder to Ignore ? Revisiting Pop-Up Fatigue and Approaches to Prevent It," in *SOUPS*. USENIX Association, 2014, pp. 105–111.

[95] "Opinion of Advocate General Szpunar in Case C-673/17, ECLI :EU :C :2019 :246 – Planet49 GmbH v Bundes verbandder Verbraucherzentralen und Verbraucher-verbände–Verbraucherzentrale Bundesverbande," 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CC0673.

[96] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein, "Sleights of privacy : framing, disclosures, and the limits of transparency," in *SOUPS*. ACM, 2013, pp. 9 :1–9 :11.

[97] R. Chatellier, G. Delcroix, E. Hary, and C. Girard-Chanudet, "Shaping choices in the digital world," 2019, https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[98] M. Toth, N. Bielova, C. Santos, V. Roca, and C. Matte, "Contribution to the public consultation on the CNIL's draft recommendation on "cookies and other trackers"," 2020. [Online]. Available : https://hal.inria.fr/hal-02490531

[99] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa : USENIX Association, Jul. 2015, pp. 1–17. [Online]. Available : https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

[100] F. Karegar, J. S. Pettersson, and S. Fischer-Hübner, "The dilemma of user engagement in privacy notices : Effects of interaction modes and habituation on user attention," *ACM Transactions and Security*, vol. 23, no. 15, p. 1–38, 2020. [Online]. Available : http://urn.kb.se/resolve?urn=urn:nbn:se:kau:diva-76844

[101] R. Hertwig and T. Grüne-Yanoff, "Nudging and boosting : Steering or empowering good decisions," *Perspectives on Psychological Science*, vol. 12, pp. 973 – 986, 2017.

[102] L. Stark, "Come on feel the data (and smell it)," 2014. [Online]. Available : https://www.theatlantic.com/technology/archive/2014/05/data-visceralization/370899/

[103] S. C. on Digital Platforms, "Privacy and data protection subcommittee report," 2019, https://research.chicagobooth.edu/-/media/research/stigler/pdfs/data---report.pdf?la=en&hash=54ABA86A7A50C926458B5D44FBAAB83D673DB412.

CHAPTER 4

Consent Management Platforms under the GDPR : processors and/or controllers ?

Cristiana Santos, Midas Nouwens, ***Michael Toth****, Nataliia Bielova and Vincent Roca*

Appeared in : Privacy Technologies and Policy – 9th Annual Privacy Forum, 2021, online.

I contributed to the analysis of additional processing activities, scanning and pre-sorting of tracking technologies, included third-party vendors, and manipulative design strategies.

Abstract

Consent Management Providers (CMPs) provide consent pop-ups that are embedded in ever more websites over time to enable streamlined compliance with the legal requirements for consent mandated by the ePrivacy Directive and the General Data Protection Regulation (GDPR). They implement the standard for consent collection from the Transparency and Consent Framework (TCF) (current version v2.0) proposed by the European branch of the Interactive Advertising Bureau (IAB Europe). Although the IAB's TCF specifications characterize CMPs as data processors, CMPs factual activities often qualifies them as data controllers instead. Discerning their clear role is crucial since compliance obligations and CMPs liability depend on their accurate characterization. We perform empirical experiments with two major CMP providers in the EU : Quantcast and OneTrust and paired with a legal analysis. We conclude that CMPs process personal data, and we identify multiple scenarios wherein CMPs are controllers.

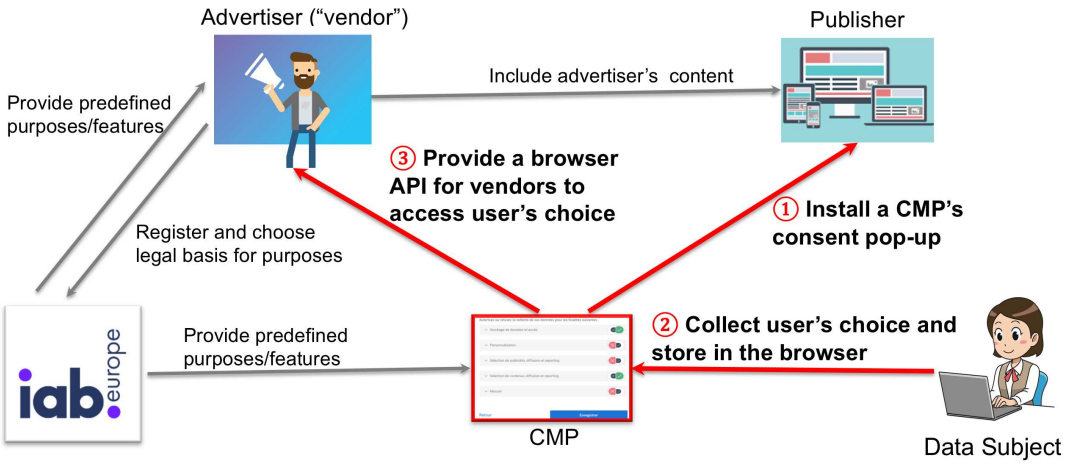


Figure 4.1 – **Actors under IAB Europe TCF ecosystem :** IAB Europe, Advertisers (called "vendors"), Consent Management Providers (CMPs), Publishers, Data Subjects. The IAB Europe defines the purposes and features that are shown to users. Registered vendors declare purposes and legal basis and the features upon which they rely. CMPs provide consent pop-up, store the user's choice as a browser cookie, and provide an API for advertisers to access this information.

4.1 Introduction

To comply with the General Data Protection Regulation (GDPR) [1] and the ePrivacy Directive (ePD) [2], a website owner needs to first obtain *consent* from users, and only then is allowed to process personal data when offering goods and services and/or monitoring the users' behavior. As a result, numerous companies have started providing "*Consent as a Service*" solutions to help website owners ensure legal compliance [3].

To standardise * the technical implementation of these consent pop-ups, the European branch of the Interactive Advertising Bureau (IAB Europe), an industry organisation made up of most major advertising companies in the EU, developed a Transparency and Consent Framework (TCF) [4]. This framework (currently on version 2.0) was developed to preserve the exchange of data within the advertising ecosystem, which now requires being able to demonstrate how, when, from who, and on which legal basis that data is collected. The actors in this ecosystem are IAB Europe, advertisers (called "vendors"), Consent Management Providers (CMPs), publishers, and data subjects (see Figure 4.1).

Although recent work has started to address the complex technical and legal aspects of the IAB Europe TCF ecosystem [5–11], *neither prior work nor court decisions* have so far discussed the role of the CMPs. Therefore, it is currently unclear what the role of these CMPs is under the GDPR, and consequently what their legal requirements and liabilities are.

This paper examines if and when CMPs can be considered a *data controller* – i.e., an actor responsible for determining the purposes and means of the processing of personal data (Art. 4(7) GDPR) – or a *data processor* – i.e., an actor which processes personal data on behalf of the controller (Art. 4(8) GDPR).

∗. Standardization is used within the meaning of streamline at scale consent implementation.

Discerning the correct positioning of CMPs is crucial since compliance measures and CMPs liability depend on their accurate characterization (GDPR Recital 79). To determine the role of CMPs under the GDPR, in this paper we answer the following research questions :

§4.2 When are CMPs processing personal data ?

§4.3 When do CMPs act as data processors ?

§4.4 When do CMPs act as data controllers ?

Note that the TCF is a voluntary framework : not all CMPs are part of it and abide by its policies. However, it has become a *de facto* standard used by a growing number of actors [5, Fig. 6]. This means that focusing on the CMPs within this ecosystem provides results that can more easily be generalised, compared to looking at the specific implementations of individual CMPs. Whenever we refer to CMPs in the rest of the article, we are referring to CMPs registered as part of the IAB Europe TCF. Our argumentation is based on :

— legal analysis of binding legal sources (GDPR and case-law) and relevant data protection guidelines from the European Data Protection Board and Data Protection Authorities, document analysis of the IAB Europe TCF,
— empirical data gathered on our own website by deploying Quantcast and OneTrust – the two most popular CMPs in the EU, found respectively on 38.3% and 16.3% of the websites with a EU or UK TLD analyzed by Hils et al. [5].

A legal analysis is done by a co-author with expertise in Data Protection Law, and a technical analysis by Computer Science co-authors.

In this paper, we make the following **contributions** :

— we conclude that CMPs process personal data,
— we analyse what exact behavior qualifies a CMP as a processor,
— we identify several scenarios wherein CMPs can qualify as controllers, and
— we provide recommendations for policymakers.

4.2 When are CMPs processing personal data ?

The *raison d'être* of CMPs is to collect, store, and share a *Consent Signal* [4, 12] of a data subject. The Consent Signal is a text-based digital representation of the user's consent in a standardised format, stored in the user's browser, and provided to third-party vendors by the CMP [4, paragraph 17, page 9]. Before discussing whether a CMP can be considered a data controller or processor, we first need to establish whether it even falls under the GDPR, which depends on whether it can be considered to process personal data. To answer this question, we first explain the definition of personal data under the GDPR, and then investigate which data CMPs process in practice and whether such data qualifies as personal data.

4.2.1 Legal definitions

Personal data is *"any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly. In particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* (Article 4(11) GDPR [1]). Recital

30 asserts that online identifiers provided by their devices, such as IP addresses, can be associated to a person, thus making them identifiable.

Processing consists of *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"* (Article 4(2) GDPR). In practice, this means that almost any imaginable handling of personal data constitutes processing [13].

4.2.2 Mapping legal definitions into practice

Consent Signal. CMPs provide a consent pop-up, encode the user's choice in a Transparency and Consent (TC) string †, store this value in a user's browser and provide an API for advertisers to access this information.

IAB Europe TCF specifies that when Consent Signal is "globally-scoped" (shared by CMPs running on different websites), the Consent Signal must be stored in a third-party cookie `euconsent-v2` set with `.consensu.org` domain.

CMPs who register at IAB Europe TCF are provided with a subdomain `<cmp-name>.mgr.consensu.org` that is "delegated by the Managing Organisation (IAB Europe) to each CMP" [14]. "Globally-scoped" Consent Signal allows all CMPs who manage content on their `<cmp-name>.mgr.consensu.org` domains to also have access to the Consent Signal that is automatically attached to every request sent to any subdomain of `.consensu.org`. As a result, other consent pop up providers, who are not registered at IAB Europe, are not in a position to receive the Consent Signal stored in the user's browser because they have no access to any subdomain of `.consensu.org`, owned by IAB Europe. For non-global consent, a CMP can freely choose which browser storage to use for Consent Signal [14]. The Consent Signal contains a non human-readable encoded version (base64 encoded) of :

— the list of purposes and features the user consented to ;
— the list of third-party vendors the user consented for ;
— the CMP identifier and version, together with other meta-data.

IP address. While the Consent Signal does not seem to contain personal data, CMPs additionally have access to the user's IP address. In order to include a consent pop-up, publishers are asked to integrate in their website a JavaScript code of a CMP (see step (1) in Figure 4.1). Such code is responsible for the implementation of a consent pop-up and in practice is loaded either : (1) directly from the server owned by a CMP (OneTrust's banner is loaded from the OneTrust's domain `https://cmp-cdn.cookielaw.org`), or (2) from the server `<cmp-name>.mgr.consensu.org` "delegated by the Managing Organisation (IAB Europe) to each CMP" [14] (Quantcast's script for consent pop-up is loaded from `https://quantcast.mgr.consensu.org`).

As an inevitable consequence of an HTTP(S) request, the server (of a CMP or controlled by a CMP via a DNS delegation by IAB Europe) is thus able to access the IP address of a visitor in this process. Additionally, CMP declare in their privacy policies the collection of IP addresses [15,16]. Therefore, from a technical point of view, a CMP is able to record the IP address of the user's terminal in order to fulfil its service. Hereby we conclude that CMPs can have access to the user's IP address. An IP address can be a cornerstone for data aggregation or identifying individuals.

†. For the sake of uniformity, we call it "Consent Signal" in the rest of the paper.

Empirical studies [17, 18] found that a user can, over time, get assigned a set of IP addresses which are unique and stable. Mishra et al. [18] found that 87% of users (out of 2,230 users over a study period of 111 days) retain at least one IP address for more than a month. 2% of user's IP addresses did not change for more than 100 days, and 70% of users had at least one IP address constant for more than 2 months. These assertions render IP addresses as a relatively reliable and robust way to identify a user. Even though these results denote IP address stability (specially static IP addresses), the data protection community and case law diverge in the understanding of "dynamic" IP addresses as personal data. An IP address would be personal data if it relates to an *identified* or *identifiable* person. It was decided [19] that a dynamic IP address (temporarily assigned to a device) is not necessarily information related to an *identified* person, due to the fact that "such an address does not directly reveal the identity of the person who owns the computer from which a website was accessed, or that of another person who might use that computer". The question that follows is *whether an IP address relates to an identifiable person for this IP address* to be considered personal data. In order to determine whether a person is *identifiable*, account should be taken of *all the means that can reasonably be used* by any entity to identify that person (Recital 26 GDPR). This risk-based approach [19, 20] means that anyone possessing the means to identify a user, renders such a user identifiable. Accordingly, CMPs have the means to collect IP addresses (as declared in their privacy policies) and to combine all the information relating to an identifiable person, rendering that combined information (IP address and, in some cases, Consent Signal) personal data.

Since identifiability of a person depends heavily on context, one should also take into account any other reasonable means CMPs have access to, for example, based on their role and market position in the overall advertising ecosystem [20]. One important aspect to consider, then, is the fact that these CMP providers can simultaneously also play a role as an advertising vendor, receiving the Consent Signal provided by their own CMP and (if positive) the personal data of the website visitor. Quantcast, for example, appears in the Global Vendor List (GVL) [21] as registered vendor #11. In the consent pop-up, their Privacy Policy [15], and their Terms of Service [22, 23], Quantcast mentions a large number of purposes for processing personal data, such as "Create a personalised ads profile", "Technically deliver ads or content", and "Match and combine offline data sources". The Evidon Company Directory [24] labels Quantcast as "Business Intelligence, Data Aggregator/Supplier, Mobile, Retargeter", and also mentions a large list of possible personal data collection from them. According to the same source, Quantcast also owns a retargeter called Struq. In view of this fact, CMPs seem to have reasonable means to combine information relating to an identifiable person, rendering that information personal data.

Summary. Although a Consent Signal itself does not seem to contain personal data, when the consent pop-up script is fetched from a CMP-controlled server, the CMP also processes the user's IP address, which the GDPR explicitly mentions as personal data. The possibility to combine both types of data renders a user identifiable. This possibility becomes particularly pertinent whenever a CMP also plays the role of a data vendor in the advertising ecosystem, which gives them access to more data that could be combined and increase the identifiability of a user.

4.3 When are CMPs data processors ?

4.3.1 Legal definitions

A **processor** is an actor that processes personal data *on behalf* of the controller (Article 4 (8) GDPR). The relevant criteria that define this role are : (i) a dependence on the controller's instructions regarding processing activities [13], (Art. 28(3)(a)), Recital 81), and ; (ii) a compliance with those instructions [25], which means they are not allowed to go beyond what they are asked to do by the controller [25].

4.3.2 Mapping legal definitions into practice

The main objectives of CMPs clearly correspond to the definition of data processors, because they act according to the instructions given by the website publisher with regards to the legal bases, purposes, special features, and/or vendors to show to the user in the consent pop-up. IAB Europe TCF also explicitly defines CMPs as data processors in the TCF documentation [4, page 10 (paragraph 8), page 11 (paragraph 11)]. The classification of the CMP as data processors is currently the widely shared consensus about their role.

Responsibility of CMPs as processors. If a CMP is established as a data processor, it can be held liable and fined if it fails to comply with its obligations under the GDPR (Articles 28(3)(f) and 32-36 GDPR). Moreover, if a false Consent Signal is stored and transmitted, it may well be considered an "unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed" [1, Art. 32(2)]. Recent works reported numerous CMPs violating the legal requirements for a valid positive consent signal under the GDPR. For example, researchers detected pre-ticked boxes [6, 8], refusal being harder than acceptance [8] or not possible at all [6], choices of users not being respected [6], as well as more fine-grained configuration barriers such as aesthetic manipulation [26, Fig. 11], framing and false hierarchy [26, Fig. 12].

4.4 When are CMPs data controllers ?

In this section we analyse when CMPs are data controllers. Firstly, in section 4.4.1 we provide the legal definitions necessary to qualify CMPs as data controllers. In the following sections (4.4.2 – 4.4.5) we will map these legal definitions into practice. Although CMPs are explicitly designated as processors by the IAB Europe TCF specifications [4], we analyse four functional activities of CMPs that enables their qualification as data controllers. We include a technical description of such activities followed by a legal analysis. These activities refer to :

- §4.4.2 Including additional processing activities in their tools beyond those specified by the IAB Europe ;
- §4.4.3 Scanning publisher websites for tracking technologies and sorting them into purpose categories ;
- §4.4.4 Controlling third-party vendors included by CMPs ;
- §4.4.5 Deploying manipulative design strategies in the UI of consent pop-ups.

Finally, in section 4.4.6 we determine the responsibility of a CMPs as data controllers.

4.4.1 Legal definitions

The primary factor defining a **controller** is that it "determines the purposes and means of the processing of personal data" (Article 4(7) GDPR). We refer to the European Data Protection Board (EDPB) opinion [13] to unpack what is meant by 1) "determines", and 2) "purposes and means of the processing of personal data".

"Determines' refers to having the "determinative influence", "decision-making power" [13,25,27] or "independent control" [28] over the purposes and means of the processing. This concept of "determination" provides some degree of flexibility (to be adapted to complex environments) and the Court of Justice of the EU (CJEU), Data Protection Authorities (DPAs) and the EDPB describe that such control can be derived from :

- professional competence (legal or implicit) [13] ;
- factual influence based on factual circumstances surrounding the processing. (e.g. to contracts, and real interactions) [13] ;
- image given to data subjects and their reasonable expectations on the basis of this visibility [13] ;
- which actor "*organizes, coordinates and encourages*" data processing [27] (paragraphs 70, 71) ;
- interpretation or independent judgement exercised to perform a professional service [28].

"Purposes" and "means" refer to "why" data is processed (purposes) and "how" the objectives of processing are achieved (means). Regarding the determination of "purposes", the GDPR merely refers that purposes need to be explicit, specified and legitimate (Article 5(1)(b) [29]. In relation to the determination of "means", the EDPB distinguishes between "essential" and "non-essential means" and provides examples thereof [13, 25] :

- "Essential means" are inherently reserved to the controller ; examples are : determining the i) type of personal data processed, ii) duration of processing, iii) recipients, and iv) categories of data subjects ;
- "Non-essential means" may be delegated to the processor to decide upon, and concern the practical aspects of implementation, such as : i) choice for a particular type of hardware or software, ii) security measures, iii) methods to store or retrieve data.

Important notes on the assessment of controllers are referred herewith. The role of controller and processor are *functional* concepts [25] : the designation of an actor as one or the other is derived from their *factual roles and activities* in a specific situation [13], rather than from their formal designation [30]. Notably, access to personal data is not a necessary condition to be a controller [31, 32]. Moreover, the control exercised by a data controller may extend to the entirety of processing at issue, and also be limited to *a particular stage in the processing* [32].

4.4.2 Inclusion of additional processing activities

Technical description. When publishers employ the services of a CMP to manage consent on their website, the CMP provides the publisher with the necessary code to add their consent solution to the website. Although this code is ostensibly only for managing consent, it is possible for the CMP to also include other functionality.

As part of our empirical data gathering, we assumed the role of website owner (i.e., publisher) and installed a QuantCast CMP [33] on an empty website. Website owners are instructed by the CMP to "copy and paste the full tag" into their website header and "avoid modifying the tag as

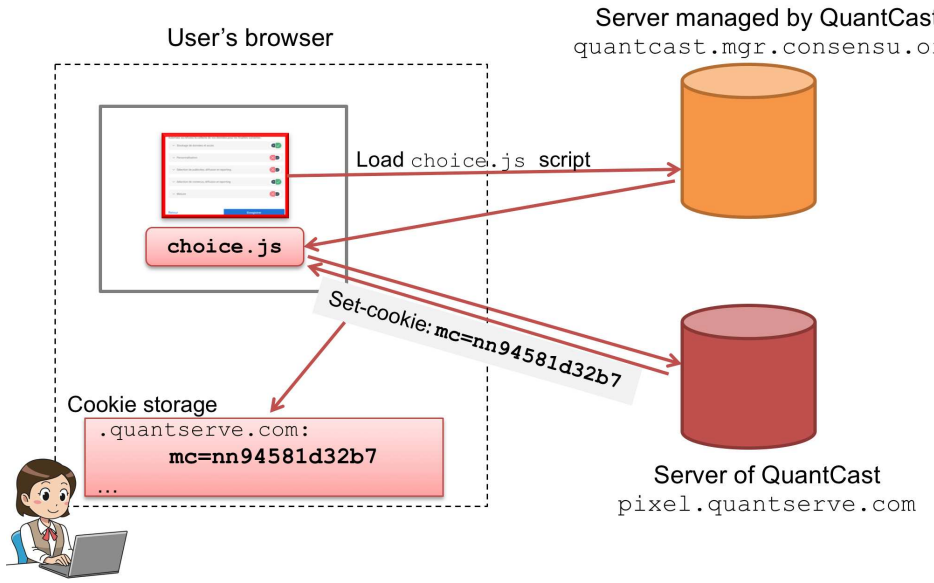


Figure 4.2 – Loading of invisible pixel by a QuantCast consent pop-up : the pixel sets a third-party cookie `mc` with a user-specific identifier that is further accessible to all subdomains of `quantserve.com`.

changes may prevent the CMP from working properly." [34] : the tag is the minimal amount of code necessary to load the rest of the consent management platform from an external source.

When installing the Quantcast CMP, we discovered that the "Quantcast Tag" script that deploys a consent pop-up on the website also loads a further script `choice.js` that integrates a 1x1 invisible image loaded from the domain `pixel.quantserve.com` (see Figure 4.2). When this image is loaded, it also sets a third-party cookie `mc` in the user's browser. By replicating the methodology to detect trackers [35], we analysed the `mc` cookie from `pixel.quantserve.com`; this cookie is *"user-specific"* – that is, its value is different for different website visitors – and comes from a third-party, allowing tracking across all sites where some content from `quantserve.com` or its subdomains is present. Such tracking by `quantserve.com` is prevalent in practice : recent research shows that third-party trackers from QuantCast are in top-10 tracking domains included by other trackers on 9K most popular websites [35, Fig. 6].

In the documentation that describes the QuantCast CMP, they mention that their CMP also contains a "QuantCast Measure" product [34] that is labeled as *"audience, insight and analytics tool"* for *"better understanding of audience"* [36]. The `mc` cookie we detected is the only cookie present on our empty website *before interacting with the QuantCast pop-up*, and thus we conclude that this cookie is likely responsible for the audience measurement purpose of QuantCast.

Legal analysis. The QuantCast script installs *both a consent pop-up and a tracking cookie*, and its technical implementation makes it impossible for website owners to split these two functionalities. Such joint functionality triggers consequences on its legal status. The tracking cookie enables the QuantCast CMP to process data for its own tracking and measurement purposes, regardless of any instructions from the publisher, nor from the specifications of the IAB Europe TCF. Hence, the

independent and determinative influence of a CMP is based on factual circumstances surrounding the processing, which qualifies a CMP in this scenario as a data controller.

4.4.3 Scanning and pre-sorting of tracking technologies

Technical description. One of the services CMPs often provide to publishers is a *scanning technology* which identifies the tracking technologies currently installed and active on the publisher's website (e.g., "first- and third-party cookies, tags, trackers, pixels, beacons and more" [37]). This scan is generally the first step when installing a consent pop-up on the website, and can be configured to automatically repeat on a regular basis.

In addition to providing descriptive statistics on the trackers currently active (e.g., what type of tracking), the scan results also include a *pre-sorting* of each of these technologies *into a particular data processing category* which are then displayed in the banner. In the case of OneTrust's CookiePro scanner, which is integrated into the banner configuration procedure when it is performed with an account, trackers are *"assigned a Category based on information in the Cookiepedia database"* [38, 39] (a service operated by OneTrust itself). The scanning includes identifying trackers (and matching them with vendors using Cookiepedia) and categorising these trackers/vendors in specific purposes. The four common purposes of trackers of Cookiepedia are i) strictly necessary (which includes authentication and user-security) ; ii) performance (also known as analytics, statistics or measurement) ; iii) functionality (includes customization, multimedia content, and social media plugin) ; and iv) targeting (known as advertising). Any trackers which cannot be found in the database are categorised as "Unknown" and require manual sorting (see Figure 4.3). From the setup guides, there seems to be no explicit or granular confirmation required by the publisher itself (although they can edit after the fact) : once the scan is complete, the categorisation of trackers is performed automatically and the consent pop-up is updated. In other words, the CookiePro's consent pop-up interface is in part automatically configured by the scanning tool.

This kind of scanning and categorising feature based on a CMPs own database is also offered by several other CMPs such as Cookiebot [40], Crownpeak [41], TrustArc [42] and Signatu [43].

Legal analysis. In this concrete scenario, through providing the additional services and tooling (besides consent management) of scanning and consequently presorting tracking technologies into pre-defined purposes of data processing, CMPs contribute to the definition of purposes and to the overall compliance of the publisher wherein the CMP is integrated. This level of control of a CMP in determining the purposes for processing personal data and means is a decisive factor to their legal status as data controllers.

Moreover, CMPs that offer this additional service can be potentially be qualified as a *joint controller* (Article 26 GDPR) together with the publisher, as both actors jointly determine the purposes and means of processing. In line with the criteria provided by the EDPB [25], these additional processing operations convey the factual indication of a pluralistic control on the determination of purposes from this concrete CMP and respective publisher embedding these services by default. The acceptance of scanning and categorization of purposes entails i) a *common and complementing* decision taken by both entities, wherein the categorization of purposes ii) is *necessary* for the processing to take place in such manner that it has a *tangible impact* on the determination of the purposes and means of the processing and on the overall and forthcoming data processing. The provision of both consent pop-up and scanning tool services by a CMP to a publisher creates a situation of *mutual benefit* [31, 32] : CMPs provide a service that creates a competitive advantage

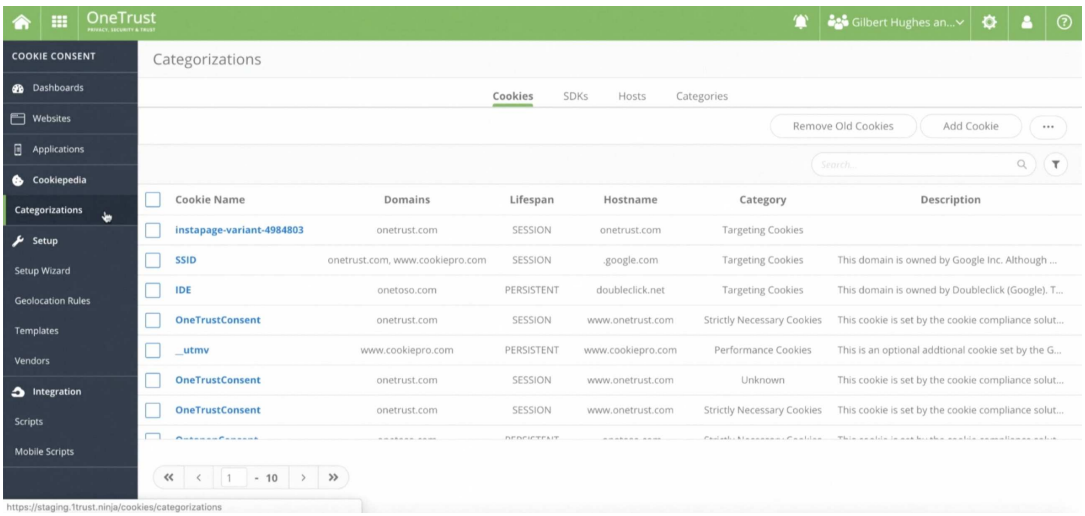


Figure 4.3 – CookiePro's configuration back-end designed for the publisher, when logged. After completing a scan for trackers on the publisher's website, this screen shows the trackers that were found together with a category they are assigned with.

compared to other CMP providers, and publishers are relieved of having to manually match trackers with vendors, purposes, and legal bases. As joint controllers, both entities would then need to make a transparent agreement to determine and agree on their respective responsibilities for compliance with the obligations and principles under the GDPR, considering also the exercise of data subjects' rights and the duties to provide information as required by Articles 13 and 14 of the GDPR. The essence of such arrangement must be made available to the data subject [25].

Such joint responsibility does not necessarily imply equal responsibility of both operators [31], nor does it need to cover all processing, in other words, it may be limited to this particular stage in the processing of scanning and presorting of trackers [32].

4.4.4 Controlling third-party vendors included by CMPs

Technical description. Upon installation of a CMP, the website publisher generally has the possibility to decide which vendors (third-party advertisers) to include in the consent pop-up. From more than 600 vendors currently registered at IAB Europe TCF [21], only the selected vendors will be then stored in the Consent Signal when the user interacts with the consent pop-up. In practice, the way the publisher effectively exercises this choice of vendors depends on the options available in the configuration tool provided by the CMP. The IAB policies explicitly state that a CMP cannot have preferential treatment for one vendor or another [4, paragraph 6(3)]. Hence, CMPs cannot pre-select or treat vendors differently, unless *a publisher explicitly asks* a CMP to include/delete some vendors from the list of all vendors.

Herewith we analyse two case studies of QuantCast and OneTrust. Figure 4.4 shows an installation process of QuantCast CMP, which gives some power to publishers. It includes by default *around 671 vendors registered in the IAB Europe TCF*, but allows a publisher to remove some of the vendors from this list. This power given to publishers is, however, limited : publishers must either manually search and *select one-by-one the vendors they want to exclude*.

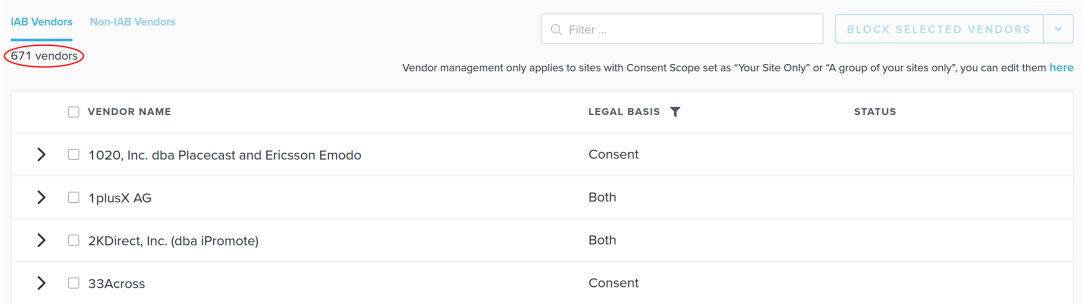


Figure 4.4 – Installation process of QuantCast CMP [Captured on 5 Feb. 2021]. A publisher has to manually search and exclude one-by-one the vendors from the list of 671 vendors registered in IAB Europe TCF.

Regarding OneTrust's free, open access service called *CookiePro Free IAB TCF 2.0 CMP Builder* [44], it gives no control to the publisher over the list of vendors to include. As a result, when the user clicks "Accept" in a CookiePro banner we installed on our empty website, the Consent Signal contains 2 special features optin, 10 purposes under the legal basis of consent, 9 purposes under legitimate interest, *631 vendors for consent*, and 261 vendors under legitimate interest.

Relying on a publisher to manually remove the vendors with whom it does not have a partnership presupposes that publishers are willing to actively check and configure the list of vendors, which can require an active action from a publisher on a separate screen during the configuration process. Such assumption contends with relevant findings from behavioral studies regarding *default effect bias*, referring to the tendency to stick to default options [45–48]. Thaler and Sunstein concluded that *"many people will take whatever option requires the least effort, or the path of least resistance"* [49]. It seems reasonable to argue that publishers will generally leave the list as is.

Legal analysis. CMPs are in a position to decide what decision-making power to award to website publishers regarding the selection of specific vendors. By restricting the ability of the publisher to (de)select vendors, the CMP obliges the publisher to present to the user the full list of IAB Europe-registered vendors. We recall that when registering to the IAB Europe, each vendor declares a number of purposes upon which it wishes to operate, and hence it can be concluded that the CMP automatically increases the number of purposes displayed to – and possibly accepted by – the end-user. As a result, a CMP requires the publisher to present more processing purposes than necessary, which has direct consequences on the interface the end-user will interact with.

With such factual decision-making power over the display of purposes rendered to users, it can be observed that CMPs exert influence over the determination of purposes of data processing, turning it to a data controller. Relatedly, deciding on the third-parties that process personal data consists on the determination of *"essential means"* – a competency allocated only to controllers, which again consolidates our conclusion that CMPs are data controllers in the above mentioned scenario.

This practice of including by default hundreds of third-party vendors implies that CMPs seem to breach several data protection principles :
Transparency and fairness principle (Article 5(1)(a) GDPR) which mandates controllers to handle data in a way that would be reasonably expected by the data subjects. When users signify their

preferences in the consent pop-up, they are not aware nor expect their data to be potentially shared with around 600 third-parties. Moreover, the inclusiveness by default of this amount of partners seems to trigger severe risks to the rights of users and thus this consent sharing needs to be limited (Recital 75 GDPR).

Minimization principle (Article 5(1)(c) GDPR) provides that data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processes". This principle is generally interpreted as referring to the need to minimise the quantity of data that is processed. One may, however, also wonder whether the principle extends to other characteristics such as the number of recipients to which data is shared with. Moreover, according to the theory of choice proliferation, a large number of purposes can lead to the user experiencing negative effects. However, in the case of consent pop-ups, the critical threshold of presented purposes beyond which these effects occur is not yet known [50].

4.4.5 Deployment of manipulative design strategies

Legal compliance vs. consent rates. When designing their consent pop-ups, CMPs have considerable freedom : The only constraint placed on them by the IAB's TCF is that they need to include the purposes and features exactly as defined by the IAB Europe [4]. From a UI perspective, CMPs thus enjoy a design space and can choose *how exactly these choices are presented to the end user*.

The primary service offered by CMPs is to ensure legal compliance, which largely determines how they exercise their design freedom. However, the advertising industry is also incentivised to strive for *maximum consent rates*. This is apparent when looking at how CMPs market themselves. For example, Quantcast describes their tool as able to "*Protect and maximize ad revenue while supporting compliance with data protection laws*" [33] and provides "Choice Reports" that detail "[h]ow many times Choice was shown, Consent rate and Bounce Rate and a detailed breakout if the full, partial or no consent given" [51]. OneTrust advertises that its CMP can "*optimize consent rates while ensuring compliance*", and "*leverage A/B testing to maximize engagement, opt-ins and ad revenue*" [52]. In other words, although the official and primary service provided by CMPs is legal compliance, in practice, their service consists in *finding the balance between strict legal compliance and maximum consent rates* (considered to be negatively correlated), and this balancing ability becomes a point of competition between them.

Manipulative design strategies in consent pop-ups. Recent works denote that many popular CMPs deploy manipulative design strategies in consent pop-ups [6, 8, 26] and that such strategies influence the users' consent decisions [8, 53]. In concrete, recent findings concernedly report the majority of users think that a website cannot be used without giving consent (declining trackers would prevent access to the website) and also click the "accept" button of the banner out of habit [53].

Technical analysis of default consent pop-ups. We portray an illustrative example of the use of manipulative design strategies in a consent pop-up. We installed a free version of OneTrust consent pop-up, the *CookiePro Free IAB TCF 2.0 CMP Builder*, on our empty website. During the installation, we chose a default version of the banner without any customization. Figure 4.5 depicts the 2nd layer of the CookiePro's default banner : the option to "Accept All" is presented on top of the banner, (hence making acceptance to all purposes prioritized), while "Reject All" and "Confirm My Choices" are located at the very bottom of the banner, only made available after scrolling down. This banner includes the dark patterns of "obstruction", "false hierarchy" and "sneaking" [54].

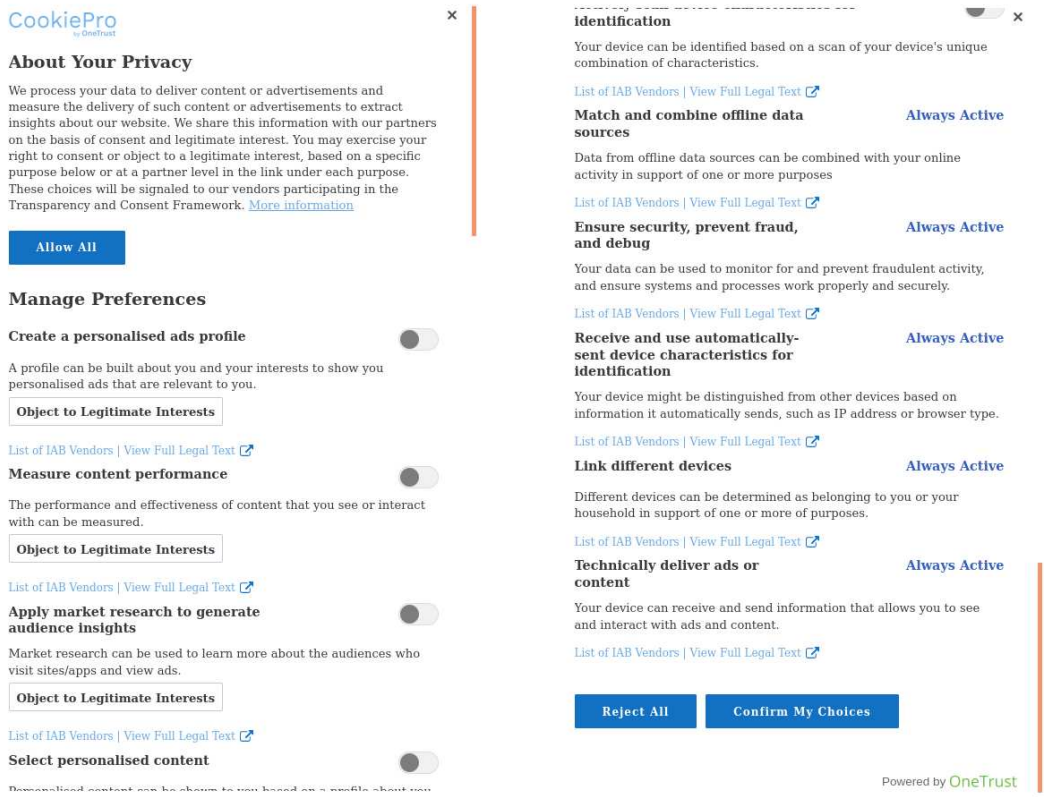


Figure 4.5 – 2nd layer of the default consent pop-up provided by CookiePro Free IAB TCF 2.0 CMP Builder (owned by OneTrust). [Captured on 13 Jan. 2021]. On the left, the top level of the page, displaying the "Accept All" button. On the right, the bottom of the same screen, displaying the "Reject All" and "Confirm My Choices" buttons, so the user needs to scroll down in order to see them.

Legal analysis. From a regulatory perspective, several guidelines have been issued by the EU Data Protection Authorities on consent pop-ups, suggesting UI should be designed to ensure that *user's choices are not affected by interface designs*, proposing a privacy by design and by default approach (Article 25 GDPR), wherein default setting must be designed with data protection in mind. Proposals of such design refer that options of the same size, tone, position and color ought to be used, so as to provide the same level of reception to the attention of the user) [55–60]. Although these guidelines are welcomed, they do not have enough legal power to be enforceable in court, and it is unclear whether they impact compliance rates. However, in practice a CookiePro default design convinces the user to select what they feel is either the only option (presented on top), or the best option (proposed in a better position), while other options (to refuse) are cumbersome and hidden.

Determination of means. The primary service of CMPs is to provide consent management solutions to publishers through consent pop-ups, and thus anything related to this service can be considered as part of the "non-essential means" that can be delegated to a processor (see Section 4.4.1). However, when CMPs decide to include manipulative design strategies – known as *dark patterns* – to increase consent optimization rate, these can be considered to go beyond their primary goal.

Manipulating users decision-making to increase the probability of prompt agreement to consent for tracking is not strictly necessary to provide its consent management service. In particular, resorting to such interface design strategies does not seem to consist of "basic features" or "service improvement" that could be considered as normally expected or compatible within the range of a processor's services [61]. In fact, there are no technical reasons that could substantiate the recourse to these dark patterns. A CMP could devise design banners in a fair and transparent way and which complies with the GDPR. The EDPB [62] refers that *"compulsion to agree with the use of personal data additional to what is strictly necessary, limits data subject's choices and stands in the way of free consent."* We conclude that the use of manipulative strategies does not qualify as a mere technical implementation or operational use to obtain lawful consent, and instead falls inside the "*essential means*" category, making them a data controller.

Determination of purposes. Following the cognition held by the CJEU on the Jehowa's Witnesses case [27], one decisive factor of the role of a controller consists in the determination of "*who organized, coordinated and encouraged*" the data processing (paragraphs 70, 71). CMPs have exclusive *judgement and control* to adopt manipulative design strategies. Such strategies have a real impact on users' consent decisions and ultimately impact the processing of their data. By deploying such strategies, CMPs do not act on behalf of any other actor (which would lead to them being recognized as "processors"), but instead have control over which purposes will be more likely to be accepted or rejected by users. In practice, CMPs' deployment of *dark patterns* that manipulate the user's final choice evidences a degree of *factual influence or decision-making power* over the processing activities that will follow.

Summary. CMPs exercise a dominant role in the decision-making power on eventual processing activities within the IAB Europe TCF ecosystem. We argue that whenever CMPs impose dark patterns to a publisher and similarly whenever CMPs propose a default banner that features dark patterns to a publisher, these facts strongly indicate a controllership status in its own right due to CMPs' influence on the determination of means and purposes of processing, even if only to a limited extent. However, the afforded discretion availed to CMPs requires a case by case analysis and is more likely to lead to divergent interpretations.

4.4.6 What is the responsibility of a CMP as controller ?

A CMP as a data processor that goes beyond the mandate given by the controller and acquires a relevant role in determining its own purposes, as shown in the scenarios in Section 4.4, becomes a controller with regard to those specific processing operations [13] and will be in breach of its obligations, hence subject to sanctions (Article 28(10)). The breadth of the parties responsibility, including the extent to which they become data controllers, should be analysed on a case by case basis [63] depending on the particular conditions of collaboration between publishers and CMPs, and then should be reflected in the service agreements.

One of their responsibilities as controllers include the obligation to comply with the principles of data protection, thereby they are required to obtain personal data fairly, lawfully and to comply with any transparency requirements with respect to users and obtain a valid consent.

Additionally, CMPs should offer design choices that are the most privacy-friendly, in a clear manner and as a default choice, in line with the principle of data protection by design and data protection by default (Article 25 of the GDPR). Finally, CMPs should respect the minimization principle – the use of compulsion methods (either in the manipulation of purposes, either pre-

registering around 600 vendors) *to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent* [62, paragraph 27].

4.5 Recommendations

In this section, based on our legal and empirical analysis, we propose a number of recommendations for policy makers that could address the current ambiguity revolving the role of CMPs.

Concepts of controller and processor in the GDPR need to be clarified. We hope to provide influential stakeholders, such as the EDPB, with operational information that can inform its next guidelines on the concepts of controller and processor in the GDPR [25]. In particular, and in the context of the current paper, we would recommend to clarify the following aspects :

1. on defining purposes in practice : our work shows that a CMP influencing users decision-making with respect to accepting or rejecting pre-defined purposes actually renders such entity co-responsible for determining purposes ;
2. on the role of deploying manipulative design in CMPs and whether this constitutes "essential means" of processing ;
3. on the contractual agreement between publishers and CMPs : such agreement should mirror as much as possible the factual roles and activities they are involved in, pursuant to legal certainty and transparency ;

Guidelines needed on "provision of services" for data processors. Data processors must limit its operations to carrying out the services for which the controller stipulated in the processing agreement. However, this design space is left to ambiguity and leeway in terms of what "providing the service" entails. Guidance is needed on what is considered to be *compatible and expected purposes* for the provision of their services/operations. For example, while security operations are surely expected, doubts remain regarding the provision of services which include other purposes that go beyond legal provisions and principles such as the compatibility between optimization of consent rate and legal compliance (as mentioned in Section 4.4.5) ; the EDPB [62, paragraph 27] mentions that such goal cannot be prioritized over the control of an individual's personal data : *an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service*.

DPAs should scale up auditing of CMPs. Currently, DPAs primarily use labour-intensive, small-sample, qualitative methods to evaluate the legal compliance of CMPs (e.g., the Irish DPA analysed consent pop-ups of 38 websites via a "desktop examination" [64]). Although our normative stance is that compliance evaluations should not be outsourced to algorithms and always involve human oversight, data-driven and automated tools could help DPAs gain a broader understanding of CMP design and compliance trends within their jurisdiction. Auditing can be automated (for example, with scraping technologies) to analyse the presence or absence of certain consent options (e.g., a reject button), interaction flows (e.g., number of clicks to access an option), or default settings (e.g., checked or unchecked choices). Not all requirements for consent are as binary and can be measured in this way (such as the quality of purpose descriptions), but gathering and continuously monitoring those aspects can provide DPAs with initial indications.

These insights can be used to decide which follow-up investigations are necessary, and also which aspects might provide the biggest impact if addressed.

Automated auditing of CMPs requires extension of consent signal. The IAB Europe has created a standardised format for consent signals and successfully implemented APIs that allow various entities to interoperate with each other. Such consent was created to simplify the exchange of the digital version of consent between CMPs and advertisers. They do not, however, contain elements that could help DPAs and users to evaluate the *validity of collected consent* through automated means. We strongly suggest these standards and APIs should be expanded (or new ones developed by neutral parties) to include information about the interface design of a consent pop-up. Such extended digital format of consent will make consent services computationally legible by more actors, such as regulators and researchers.

Additionally, in the current IAB Europe TCF system, third-party advertisers (vendors) just receive a Consent Signal as a part of HTTP(S) request or via browser APIs, but there is no proof whether such Consent Signal is valid and whether a vendor actually received it (or, for example, did not generate it by itself instead). We recommend IAB Europe TCF to change this practice and to propose solutions that demonstrate evidence of consent collection and its integrity.

Guidance needed on validity of pre-registration of vendors. Through our analysis, we identified that CMPs have the capability to "pre-register" about 600 vendors during the installation process on a website. This pre-registration of vendors means that if the user accepts some of the purposes presented in the consent pop up, then all the vendors will be automatically added to a Consent Signal (see an example of OneTrust in section 4.4.4, where 632 vendors are allowed when the user clicks "Accept"). Consent stored by CMP in this case *pre-authorizes* processing of personal data for around 600 vendors, even if those vendors are not present on the website, thus making consent being collected *for future and unforeseen potential processing*. Therefore, such practice may violate the principles of transparency, fairness and minimization principles. We hope our analysis of the IAB Europe TCF and the capability of CMPs to pre-register vendors that do not yet process personal data, will help policy makers to provide further guidance on the validity of such practice.

Further recommendations are needed due to the decision-making power of consent pop-up providers. In this article, we have analysed two most popular CMPs in the EU – QuantCast and OneTrust– and detected several scenarios when consent pop-up providers can be considered data controllers due to the enormous power of CMPs that can inject any type of additional functionality at any time in the banner, without the publisher being in position to technically know or oppose to it. We hope that policy makers take these scenarios into account and provide recommendations for such providers (either withing or outside of IAB Europe TCF) identifying which practices render them as data controllers and in which conditions they will be recognized as data processors.

4.6 Related work

Previous work analysing the role of CMPs in the advertising ecosystem have examined its technical functioning and interaction designs related to the applicable regulation, but have not inquired how they relate to their role as processors or controllers under the GDPR.

Degeling et al. [10] monitored the prevalence of CMPs on websites from January 2018 until May, when the GDPR came into effect, and measured an overall increase from 50.3% to 69.9% across all 28 EU Member States. Taking a longer view, Hils et al. [5] showed how the rate of adoption doubled year over year between June 2018 and 2020, and that CMPs are mostly used by moderately popular websites (albeit with a long tail of small publishers). Nouwens et al. [8] studied the use of dark patterns in the five most popular CMPs in the UK and estimated that only 11.8% of banners meet minimum legal requirements for a valid consent (reject as easy as accept, no pre-checked boxes, and no implied consent).

Focusing on the programmatic signals rather than user behaviour, Matte et al. [6] analysed 28,000 EU websites and found that 141 websites register positive consent even if the user has not made their choice and 27 websites store a positive consent even if the user has explicitly opted out. Additionally, Matte et al. [7] discuss the purposes and legal basis pre-defined by the IAB Europe and suggest that several purposes might not be specific or explicit enough to guarantee a valid legal basis, and that a large portion of purposes should require consent but are allowed by the TCF to be gathered on the basis of legitimate interest.

Data protection authorities across EU Member States have also reacted to the role and responsibility of CMPs, and issued various guidances. The Spanish DPA [60] asserts that as long as CMPs comply with the requirements for consent, they shall be deemed an appropriate tool. It recommends that CMPs " *must be submitted to audits or other inspections in order to verify that (...) requirements are complied with*". The Irish DPA [59] reiterates CMPs should be careful to avoid non-compliant designs already explicated as part of GDPR texts (e.g., pre-ticked boxes) and emphasises their accountability and transparency obligations (i.e., consent records) The Danish DPA asserts that whenever any entity integrates content from any third party (including CMPs), it is particularly important to be aware of its role in relation to its processing of personal data that takes place [65].

4.7 Conclusion

In this paper we discussed the requirements for CMPs to be qualified as processors and as controllers and concluded that such status has to be assessed with regard to each specific data processing activity. From an empirical analysis we concluded that CMPs assume the role of controllers, and thus should be responsible for their processing activities, in four scenarios : i) when including additional processing activities in their tool, ii) when they perform scanning and presorting of tracking technologies, iii) when they include third-party vendors by default, and finally iv) when they deploy interface manipulative design strategies.

Acknowledgements

We would like to thank Daniel Woods, Triin Siil, Johnny Ryan and anonymous reviewers of ConPro'21 and APF'21 for useful comments and feedback that has lead to this paper. This work has been partially supported by the ANR JCJC project PrivaWeb (ANR-18-CE39-0008) and by the Inria DATA4US Exploratory Action project.

Bibliography

[1] "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) (text with eea relevance)," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679.

[2] "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136, accessed on 2019.10.31.

[3] C. Santos, N. Bielova, and C. Matte, "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*, pp. 91–135, 2020. [Online]. Available : https://doi.org/10.26116/techreg.2020.009

[4] IAB Europe, "IAB Europe Transparency & Consent Framework Policies," 2020, https://iabeurope.eu/wp-content/uploads/2020/11/TCF_v2-0_Policy_version_2020-11-18-3.2a.docx-1.pdf.

[5] M. Hils, D. W. Woods, and R. Böhme, "Measuring the Emergence of Consent Management on the Web," in *ACM Internet Measurement Conference (IMC'20)*, 2020.

[6] 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," in *IEEE Symposium on Security and Privacy (IEEE S&P 2020)*, 2020.

[7] C. Matte, C. Santos, and N. Bielova, "Purposes in IAB Europe's TCF : which legal basis and how are they used by advertisers ?" in *Annual Privacy Forum, APF*, ser. Lecture Notes in Computer Science, 2020, https://hal.inria.fr/hal-02566891.

[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 *CHI*, 2020.

[9] H. Pawlata and G. Caki, "The Impact of the Transparency Consent Framework on current Programmatic Advertising Practices," 2020, 4th International Conference on Computer-Human Interaction Research and Applications.

[10] 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," in *Network and Distributed Systems Security Symposium*, 2019.

[11] N. Bielova and C. Santos, "Call for Feedback to the EDPB regarding Guidelines 07/2020 on the concepts of controller and processor in the IAB Europe Transparency and Consent Framework," 2020, http://www-sop.inria.fr/members/Nataliia.Bielova/opinions/EDPB-contribution-controllers-processors.pdf.

[12] I. Europe, "Transparency and consent string with global vendor & CMP list formats (final v.2.0) : About the transparency & consent string (TC String)," 2020,

https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md#about-the-transparency--consent-string-tc-string, accessed on 14 January 2021.

[13] 29 Working Party, "Opinion 1/2010 on the concepts of "controller" and "processor" WP 169," 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[14] IAB Europe, "Transparency and Consent String with Global Vendor and CMP List Formats (Final v.2.0)," 2019, https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IABTechLab-Consentstringandvendorlistformatsv2.md, accessed on 12 February 2021.

[15] Quantcast, "Quantcast Privacy Policy," 2020, https://www.quantcast.com/privacy/.

[16] OneTrust, "OneTrust Privacy Overview," https://www.onetrust.com/privacy/.

[17] G. Maier, A. Feldmann, V. Paxson, and M. Allman, "M. : On Dominant Characteristics of Residential Broadband Internet Traffic," in *In : Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, 2009, pp. 90–102.

[18] V. Mishra, P. Laperdrix, A. Vastel, W. Rudametkin, R. Rouvoy, and M. Lopatka, "Don't count me out : On the relevance of IP address in the tracking ecosystem," in *WWW '20 : The Web Conference 2020, Taipei, Taiwan, April 20-24, 2020*, Y. Huang, I. King, T. Liu, and M. van Steen, Eds. ACM / IW3C2, 2020, pp. 808–815. [Online]. Available : https://doi.org/10.1145/3366423.3380161

[19] Court of Justice of the European Union, "Case 582/14 – Patrick Breyer v Germany," 2016, ECLI :EU :C :2016 :779.

[20] M. Finck and F. Pallas, "They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR," *International Data Privacy Law*, vol. 10, 2020.

[21] IAB Europe, "Vendor List TCF v2.0," 2020, https://iabeurope.eu/vendor-list-tcf-v2-0/.

[22] Quantcast, "Quantcast Choice Terms of Service," 2020, https://www.quantcast.com/legal/quantcast-choice-terms-of-service/.

[23] ——, "Quantcast Measure and Q for Publishers Terms of Service," 2020, https://www.quantcast.com/legal/measure-terms-service/.

[24] Evidon, "Quantcast-related pages on Evidon Company Directory," 2017, https://info.evidon.com/companies?q=Quantcast [Consulted on Jan. 8th, 2021.].

[25] European Data Protection Board, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0," 2020, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[26] 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 *ACM CHI 2021*, 2020, https://arxiv.org/abs/2009.10194.

[27] European Court of Justice, "Case 25/17 Jehovan todistajat, ECLI :EU :C :2018 :551."

[28] Information Commissioner's Office, "Data controllers and data processors : what the difference is and what the governance implications are," 2018, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/.

[29] I. Fouad, C. Santos, F. Al Kassar, N. Bielova, and S. Calzavara, "On Compliance of Cookie Purposes with the Purpose Specification Principle," in *2020 International Workshop on Privacy Engineering, IWPE*, 2020, https://hal.inria.fr/hal-02567022.

[30] Advocate General Mengozzi, "Opinion of Advocate General Mengozziin Jehovah's witnesses, C-25/17, ECLI :EU :C :2018 :57, paragraph 68," 2018.

[31] European Court of Justice, "Case C-210/16 Wirtschaftsakademie Schleswig-Holstein, ECLI :EU :C :2018 :388."

[32] ——, "Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, ECLI :EU :C :2019 :629."

[33] Quantcast, "Quantcast Choice," 2020, https://www.quantcast.com/products/choice-consent-management-platform/.

[34] ——, "Quantcast Choice - Universal Tag Implementation Guide (TCF v2)," 2021, https://help.quantcast.com/hc/en-us/articles/360052746173-Quantcast-Choice-Universal-Tag-Implementation-Guide-TCF-v2-.

[35] I. Fouad, N. Bielova, A. Legout, and N. Sarafijanovic-Djukic, "Missed by filter lists : Detecting unknown third-party trackers with invisible pixels," *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2020, 2020, published online : 08 May 2020, https://doi.org/10.2478/popets-2020-0038.

[36] Quantcast, "Quantcast Measure," 2021, https://www.quantcast.com/products/measure-audience-insights/.

[37] CookiePro, "Scanning a Website," Nov 2020, https://community.cookiepro.com/s/article/UUID-621498be-7e5c-23af-3bfd-e772340b4933.

[38] ——, "Lesson 3 : Scan Results and Categorizing Cookies," Jul 2020, https://community.cookiepro.com/s/article/UUID-309d4544-c927-fe00-da50-60ed7668c6b5.

[39] "Cookiepedia Official website," https://cookiepedia.co.uk/.

[40] Cookiebot, "Cookie scanner – revealer of hidden tracking," Sep 2020, https://www.cookiebot.com/en/cookie-scanner/.

[41] Crownpeak, "Vendor categories," n.d., https://community.crownpeak.com/t5/Universal-Consent-Platform-UCP/Vendor-Categories/ta-p/665.

[42] TrustArc, "Cookie Consent Manager," n.d., https://trustarc.com/cookie-consent-manager/.

[43] Signatu, "Trackerdetect," n.d., https://signatu.com/product/trackerdetect/.

[44] CookiePro by OneTrust, "CookiePro Free IAB TCF 2.0 CMP Builder," n.d., https://www.cookiepro.com/iab-tcf-2-builder/.

[45] E. J. Johnson, S. Bellman, and G. L. Lohse, "Defaults, Framing and Privacy : Why Opting In-Opting Out," *Marketing Letters*, vol. 13, pp. 5–15, 2002.

[46] E. J. Johnson and D. G. Goldstein, "Do Defaults Save Lives ?" *Science*, vol. 302, pp. 1338–1339, 2003.

[47] Jared Spool, "Do users change their settings ?" 2011, https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/.

[48] "Deceived by design : How tech companies use dark patterns to discourage us from exercising our rights to privacy," 2018, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design.

[49] R. H. Thaler and C. R. Sunstein, *Nudge : Improving Decisions About Health, Wealth, and Happiness*. Yale University Press, 2008.

[50] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems : A user study of consent dialogs after GDPR," in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020, pp. 481–498.

[51] Quantcast, "Quantcast Choice - User Guide," 2020, https://help.quantcast.com/hc/en-us/articles/360052725133-Quantcast-Choice-User-Guide.

[52] "OneTrust PreferenceChoice : Consent management platform (cmp)," https://www.preferencechoice.com/consent-management-platform/, accessed on January 20, 2021.

[53] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed Consent : Studying GDPR Consent Notices in the Field," in *Conference on Computer and Communications Security*, 2019.

[54] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The Dark (Patterns) Side of UX Design," in *Proceedings of the CHI Conference Human Factors in Computing Systems*, 2018, p. 534.

[55] Commission Nationale de l'Informatique et des Libertés (CNIL), "Shaping Choices in the Digital World," 2019, https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[56] Commission Nationale de l'Informatique et des Libertés (French DPA), "French guidelines on cookies : Deliberation No 2020-091 of September 17, 2020 adopting guidelines relating to the application of article 82 of the law of January 6, 1978 amended to read and write operations in a user's terminal (in particular to "cookies and other tracers")," 2020, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042388179.

[57] Greek DPA (HDPA), "Guidelines on Cookies and Trackers," 2020, http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=84,221,176,170,98,24,72,223.

[58] Information Commissioner's Office, "Guidance on the use of cookies and similar technologies," 2019, https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf.

[59] Data Protection Commission (Irish DPA), "Guidance note on the use of cookies and other tracking technologies," 2020, https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf.

[60] Agencia Española de Protección de Datos (Spanish DPA), "Guide on use of cookies," 2021, https://www.aepd.es/sites/default/files/2021-01/guia-cookies-en.pdf.

[61] M. Hintze, "Data controllers, data processors, and the growing use of connected products in the enterprise : Managing risks, understanding benefits, and complying with the gdpr," *Cybersecurity*, 2018.

[62] European Data Protection Board, "Guidelines 05/2020 on consent, Version 1.1, adopted on 4 May 2020," 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[63] Article 29 Working Party, "Opinion 2/2010 on online behavioural advertising (WP 171)," 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf.

[64] Data Protection Commission (Irish DPA), “Report by the DPC on the Use of Cookies and Other Tracking Technologies ,” 2020, https://www.dataprotection.ie/en/news-media/press-releases/report-dpc-use-cookies-and-other-tracking-technologies.

[65] Danish DPA (Datatilsynet), “Guide on consent,” www.datatilsynet.dk/media/6562/samtykke.pdf, 2019.

CHAPTER 5

On dark patterns and manipulation of website publishers by CMPs

***Michael Toth**, Nataliia Bielova and Vincent Roca*

Appeared in : Proceedings on Privacy Enhancing Technologies Symposium, July 2022, Sydney, Australia / online.

I contributed to the installation of the consent management solutions on the dedicated website, the analysis of the network communications of the services, the identification of unethical choices, and the scanner analysis.

Abstract

Web technologies and services widely rely on data collection via tracking users on websites. In the EU, the collection of such data requires user consent thanks to the ePrivacy Directive (ePD), and the General Data Protection Regulation (GDPR). To comply with these regulations and integrate consent collection into their websites, website publishers often rely on third-party contractors, called Consent Management Providers (CMPs), that provide consent pop-ups as a service. Since the GDPR came in force in May 2018, the presence of CMPs continuously increased. In our work, we systematically study the installation and configuration process of consent pop-ups and their potential effects on the decision making of the website publishers. We make an in-depth analysis of the configuration process from ten services provided by five popular CMP companies and identify common unethical design choices employed. By analysing CMP services on an empty experimental website, we identify manipulation of website publishers towards subscription to the CMPs paid plans and then determine that default consent pop-ups often violate the law. We also show that configuration options may lead to non-compliance, while tracking scanners offered by CMPs manipulate publishers. Our findings demonstrate the importance of CMPs and design space offered to website publishers, and we raise concerns around the privileged position of CMPs and their strategies influencing website publishers.

5.1 Introduction

While website publishers rely on data for statistics, advertising, monetisation, and optimisation of their websites, they tend to include tracking services in their websites. The ePrivacy Directive [1], amended in 2009 [2], and soon to be transformed into a Regulation, requires *user's consent* before any access or storage of any non-mandatory data, and hence any tracking technology, on the user's device. The European Union's General Data Protection Regulation (GDPR) [3], which went into effect on May 25, 2018, defines the rules on *valid consent* [3, Art. 4, 7]. Requirement for collecting consent on websites resulted in appearance of *consent pop-ups*, often referred to as "cookie banners", and such pop-ups have become increasingly popular among the EU-based websites [4, 5].

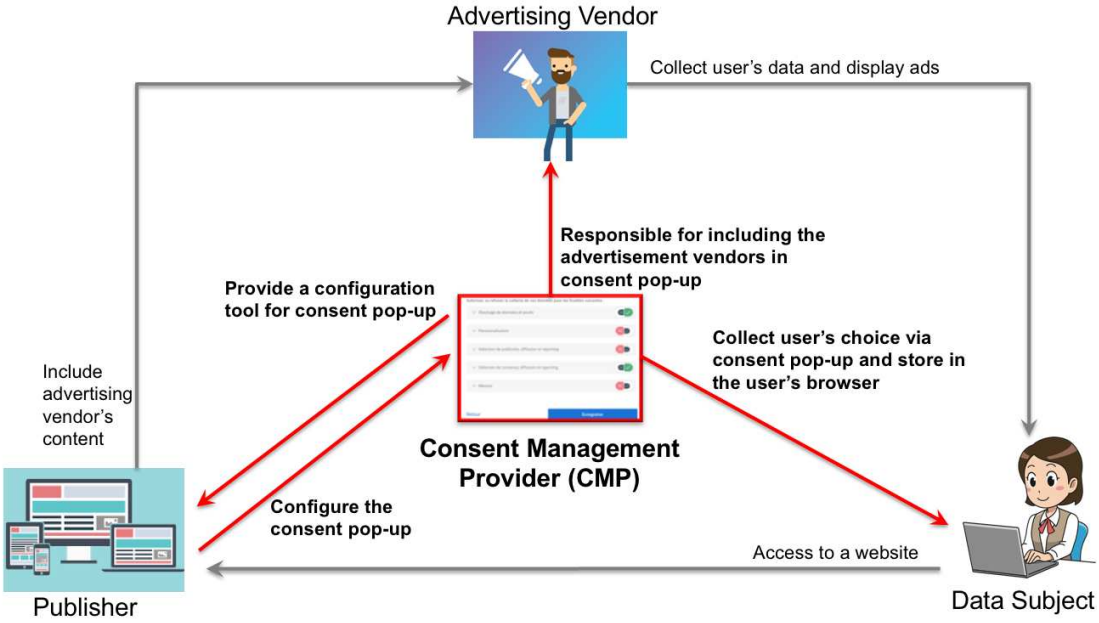


Figure 5.1 – **Influence of CMPs on the main actors in the web advertising ecosystem : publishers, advertisers, and users.** Figure inspired by the work of Santos et al. [6].

However, providing *legally-valid consent pop-up* to website users is a complex task as recently shown by Santos et al. [7], who identified 22 legal and technical requirements of valid consent on the Web based on legal sources, recommendations, and technical analysis. Collecting invalid consent have significant negative consequences for end users, such as unintentional sharing of personal information. As a result, the website publishers, who are considered legally responsible for compliance of their websites can face administrative fines up to 20 million euros, or up to 4% of the total worldwide annual turnover [3, Art. 83(5)], but also can suffer in terms of bad reputation and loss of trust. In the last two years, a number of website publishers were fined for *non-compliance* with the GDPR consent requirements on their websites as established by the EU Court of Justice in 2019 Planet49 case [8], as well as many EU Data Protection Authorities (DPAs) such as Dutch DPA [9], Spanish DPA [10], Danish DPA [11], French DPA [12–15]. Recently, in May 2021 the French Data Protection Authority (CNIL) has notified twenty popular websites in France of their violation of the EU law in the consent pop-ups on their websites [16].

As a result, website publishers often do not collect consent themselves, but prefer to delegate this task to privacy experts. This demand created a market need and opened a new business opportunity to emerging companies called Consent Management Providers (CMPs) that provide "*Consent as a Service*" solutions to website publishers. Such companies are becoming more and more popular, as demonstrated by the work of Hils et al. [17] : the usage of CMPs by websites has increased several times since the GDPR came into force on May 25, 2018. CMPs studied in most of the previous works [5, 6, 17–19] implement a common framework provided by the European branch of the Interactive Advertising Bureau (IAB Europe), called Transparency and Consent Framework (TCF) [20].

Previous works [5, 6, 19] demonstrated that CMPs occupy a specific, and rather central place in the web advertising ecosystem, as shown in Figure 5.1. Multiple studies analyzed how end users are manipulated towards giving their consent to collection of their data via consent pop-up interface, identifying *dark patterns* and other strategies and their impact on users' decision making [18, 21–24], often designed by the CMPs.

What was not studied so far, is the user journey of website publishers when they try to install the consent pop-ups provided by the CMPs : do CMPs *influence website publishers* ? Are website publishers also *manipulated towards a specific design of consent pop-ups* to be installed on their websites ? Moreover, do CMPs profit from such a central position and *collect users' data by their own services* as recently shown [6] ? Such manipulation and integration can have a significant impact on the overall compliance of the website in question. Since from legal perspective website publishers are considered "data controllers" [6] in the scope of the GDPR, website publishers are legally responsible for the overall behavior and legal compliance of their websites, even when they use third party services, such as CMPs.

In this paper, we systematically study design properties of the installation and configuration process of consent pop-ups and their potential effects on the decision making of the website publishers. We make an in-depth analysis of the configuration process from ten services provided by five popular CMP companies and identify common dark patterns employed. Our research goal is to explore the design space for consent pop-up generation process to learn how to encourage website publishers to install a legally compliant consent pop-up mechanism. We conduct a study of consent pop-up services accessible to website publishers, by installing them on our empty experimental websites, registering and analysing all steps during installation and configuration processes, detecting dark patterns in the sense of Mathur et al. [25], evaluating overall compliance of pop-ups provided by default, and monitoring network communications to identify when consent pop-ups collect users' data for their own purposes.

The study contains four distinct investigations motivated by the following research questions. We first study the presence of dark patterns in the registration and configuration process of consent pop-ups ; evaluate whether dark patterns of the default pop-up make the final pop-up compliant with the law ; and study whether CMPs use their position and large presence to collect data for their own use :

— **RQ1.** Do CMPs use ethically and/or legally problematic strategies known as "dark patterns" in the generation process of their consent pop-ups, to influence the publisher in their own interest ?

— **RQ2.** Is a consent pop-up generated with the default options provided by the CMP compliant with EU legal requirements ?

— **RQ3.** Do the default configuration options of consent pop-ups encourage publishers to comply with the requirements for collecting legally valid consent ?

— **RQ4.** What are the functionalities and the impacts of tracker scanners provided by CMPs, regarding legal compliance, role of CMPs, and publishers behaviour ?
— **RQ5.** Are CMPs abusing their central and privileged position and their presence on a large number of websites to collect data for their own use ?

The central role of CMPs and the requirements for valid consent lead us to question the influence and potential manipulation techniques used by CMPs to nudge website publishers toward selecting the most advantageous options for the CMPs. While previous work tries to categorize the existing dark patterns, and measure their presence and impact on the behaviour of final users, no work so far analyzed how publishers can be influenced by the design choices in the installation and configuration process of consent pop-ups. In this article, we focus on the influence that CMPs can have on website publishers and their impact on the entire ecosystem.

Our work contains the following contributions :

— our work is the first to perform an *in-depth analysis of the configuration process* of consent pop-ups from the website publisher perspective by ten services provided by five popular CMP companies ;
— we *identify manipulation of website publishers towards subscription to the CMPs paid plans* ; installation of consent pop-ups that do not respect the freedom of choice, such as *consent walls* [24] ;
— by carefully analysing default consent pop-ups, we *detect integration of hundreds of advertising vendors*, registered in the IAB Europe TCF (i.e., the whole Global Vendors List) which makes it hard for website publisher to remove ;
— we *identify lack of guidance for website publisher in the usage of "tracker scanner" services* provided by CMPs that impact the overall compliance of the consent pop-up and hence of the website in question. Moreover, we detect scanners that *use manipulative techniques*, such as fear of non-compliance, to nudge publishers toward subscribing to paid plans ;
— finally, we detect CMPs that *include analytic services* in the consent pop-up or scanning report for *the data collection and further exploitation of end users' data for CMPs' own purposes*.

Based on the results of our study, we open a discussion on role and power of CMPs and conclude that not only did they not improve user privacy overall, but that they could create new important issues, such as the addition of new trackers, and sometimes use manipulative design techniques in their own economic interest.

5.2 Related work

This section lists the major related works dealing with consent management process, classification and legal definition of dark patterns applied to data protection and consent, user studies and automated measurements focusing on CMPs or the IAB TCF Framework.

Measurement studies on prevalence of CMPs. In 2019, Nouwens et al. [18] studied five popular CMPs according to UK data provided by the advertising company Adzerk (now renamed Kevel) [26], and the impact of the design of consent pop-ups on the requirement for "freely given" consent. They found almost 90% of consent pop-up didn't meet the minimal legal requirements,

and the absence of a "refuse" button on the first layer of the consent pop-up increases positive consent by about 22 percentage points. Hils et al. [17] analyzed 4.2 million domains between June 2018 and 2020 in order to measure CMP adoption over time. They estimate that CMPs prevalence on websites has doubled in 2019 and again in 2020, in particular on mildly-popular websites, as a result of compliance with the EU data protection regulation. Degeling et al. [4] monitored the prevalence of CMPs on websites during the five month before the GDPR came into force. They measured an overall increase from 50.3% to 69.9% across all 28 EU Member States, and a 16% increase in consent pop-ups' adoption before and after the GDPR. Complementary to these studies, Santos et al. [6] analysed the legal role of CMPs under the GDPR : they studied in which cases CMPs were determining purposes and means of the processing, which would qualify them as data controllers.

Classification of dark patterns. Brignull [27] coined dark patterns ten years ago as a generic term to describe deceptive design of a User Interface (UI), made to influence users and their decision-making abilities. He also built the first taxonomy of these designs with examples. Gray et al. [28] further presented a broader categorization of Brignull's taxonomy and clustered these dark patterns into five categories : Nagging, Obstruction, Sneaking, Interface Interference and Forced Action. Chromik et al. [29] discuss dark patterns of explainability, transparency and control, focusing on intelligent systems. They conclude that the legal right to explanation provided by the GDPR is not sufficient, and advocates for "specific guidelines and standards". All these classifications also address the manipulative design only by testing pop-ups displayed to end-users.

Impact of dark patterns in consent pop-up interfaces on users' choices. Nouwens et al. [18] were the first to study the presence of dark patterns in the user interface of five popular CMPs, as well as a user study with 40 participants evaluating the effect of specific design on users' consent choices. Utz et al. [21] studied the influence of common graphical nudges such as changes in the position or color of the consent pop-up on more than 80,000 visitors of a German e-commerce website.

Luguri et Strahilevitz [23] did a large-scale experiment to compare the influence of "mild" and "aggressive" dark patterns on different categories of American consumers. They found "mild" dark patterns to generate less negative feelings, and less educated people to be more influenced. In 2021, Gray et al. [24] highlight connections between HCI, design, privacy and data protection on consent pop-ups, focusing on three different types of dark patterns and their influence on end users.
Mathur et al. [25] use the combined approaches of psychology, economics, ethics, philosophy, and law to formulate a general definition of dark patterns and their effects on users. Machuletz and Böhme [30] set up a user study on 150 Austrian students. They evaluated the impacts of the number of options and the presence or absence of a "Select all" button in post-GDPR consent pop-ups. Soe et al. [31] manually collected banners from 300 Scandinavian and English-speaking news services, they found wide presence of "unethical practices". In particular, 43% of the tested websites containing dark patterns were using obstruction, and 45.3% were using interface interference.

Summary. All the previous works focus on the influence of dark patterns on *end-users*. However, no studies so far have evaluated whether CMPs include manipulative practices or dark patterns that *nudge website publishers* towards installing a particular design of their consent pop-up services.

5.3 Methodology

CMP	Contact details	Installation results
CookiePro by OneTrust	OneTrust declined to give access to trial version of its paid service for academic research, but we successfully installed the two free services and later the standard paid service of their CookiePro brand.	Paid service : ✓ Free (logged) serv. : ✓ Free (unlogged) serv. : ✓
Quantcast	Free service called "Choice" was successfully installed.	Free service : ✓
TrustArc	The company did not respond in the span of one month.	Paid (Premium) serv. : ×
Cookiebot	Installation through the company website was accessible without any additional requirement. Both free and paid services were successfully installed.	Paid ✓ Free service : ✓
Crownpeak	First the company did not respond in the span of one month. Then, they added an online subscription to their website, giving us the possibility to install the "Business" service.	Paid (Premium) serv. : ✓
LiveRamp	Company scheduled an online meeting, but declined to provide its service for academic research motivating that their service was "only for publishers". The company did not recontact within one month after the meeting.	Unknown ×
Cookie Script	Installation through the company website was accessible without any additional requirements. Free and paid services were successfully installed.	Paid (Plus) serv. : ✓ Paid (Lite) serv. : ✓ Free service : ✓

Table 5.1 – **Preselected list of 7 CMPs identified via prior work [17, 18] and commercial service [32], with contact details, in particular when a direct contact with the CMP team is needed to install the service, and installation results : ✓ or × .** When a service is an order of magnitude more expensive than the average, it is labeled as "Premium".

Selection of Consent Management Providers (CMPs). To decide which CMPs to investigate, we used the most recent work in the field. Hils et al. [17] showed that Quantcast and OneTrust are the two most popular CMPs in the EU and in the US. Their presence was found respectively on 38.3% and 16.3% of the websites with a EU or UK TLD [17, Fig. 6], followed by TrustArc, Cookiebot, and Crownpeak. These five identified CMPs were also examined by the recent work of Nouwens et al. [18] and resulting as most popular in the latest version of the Kevel CMP tracker [32], a prevalence ranking service that was used by Nouwens et al. [18]. Therefore, we

have build a preliminary list of five companies – Quantcast, OneTrust, TrustArc, Cookiebot, and Crownpeak – based on previous work and Kevel service. We then added LiveRamp CMP [33], already studied by Hils et al. because of its novelty, which is linked to a major data broker [34]. Finally, we interviewed with a Data Protection Officier (DPO) who works for EU and US companies : they pointed us to Cookie Script CMP [35], which is particularly popular among Small and Medium Enterprises (SME). We preselected both free and paid services, including "premium" ones (see Table 5.1).

Installation of preselected CMPs. We contacted six of the identified companies – Quantcast, OneTrust, TrustArc, Cookiebot, Crownpeak, LiveRamp – via their websites using contact forms or provided emails, and received different types of responses. Quantcast replied that their paid CMP was discontinued, and that all the functionalities were now integrated into the free one [36]. OneTrust did a presentation call with us, but after that declined to give us access to their trial version for research purposes. However, we studied three versions of their self-service CookiePro brand, accessible via online subscription : free unlogged (no account), free logged (with mandatory account), and paid standard service. TrustArc took more than one month to reply, which prevented us to include the study of their consent pop-ups in this work. Crownpeak initially did the same, and then added an online subscription option for their "Business" CMP service, that we successfully installed. During a presentation call, LiveRamp said they would come back to us to say if it was possible to test their service that was "only for publishers", but they failed to do so after six weeks. Cookiebot and Cookie Script CMP services were directly available on the website and we installed their consent pop-ups directly. We studied both the free and paid versions of Cookiebot. For Cookie Script, we studied three services : the free version, plus the cheapest (Lite) and most expensive (Plus) paid versions.

Summary of selected CMPs. After removing the CMPs that refused installation for research purposes or did not respond in one month, we obtained ten different services provided by five CMPs : Quantcast, CookiePro, Cookiebot, Cookie Script, and Crownpeak (Table 5.2). For our analysis of the registration process (further described in Section 5.4.1), we also used results from some of the preselected CMPs to highlight their manipulative strategies during the registration.

Configuration used for experiments. For our tests, we used a dedicated version of Mozilla Firefox (v84.0) with an independent profile [37], running on GNU/Linux Ubuntu 18.04.5 LTS. To avoid interpretation errors resulting from different browser versions, we blocked automated updates of the used browser. We have also enabled all third-party cookies and disabled the "Enhanced Tracking Protection" of Firefox to avoid interference with our experiments. We install the extension Ernie [38] on this browser, that is able to detect 6 categories of cross-site tracking via cookies, including several types of cookie synchronizations. This extension, that implements cookie-based tracking detection proposed by Fouad et al. [39], enables us to detect and flag cookies according to their behaviour.

We performed our first measurements in April and May 2021, from a French institution. We did a second group of measurements between September and November 2021, in which one paid version of CookiePro, the two paid versions of CookieScript, and Crownpeak were added. In all cases, the new rules regarding the terms and conditions for refusing consent were already enforced by the French DPA, since they came in force on April 1^{st}, 2021 [40]. In other words, publishers must offer to the users the possibility of accepting and refusing read and/or write operations, such

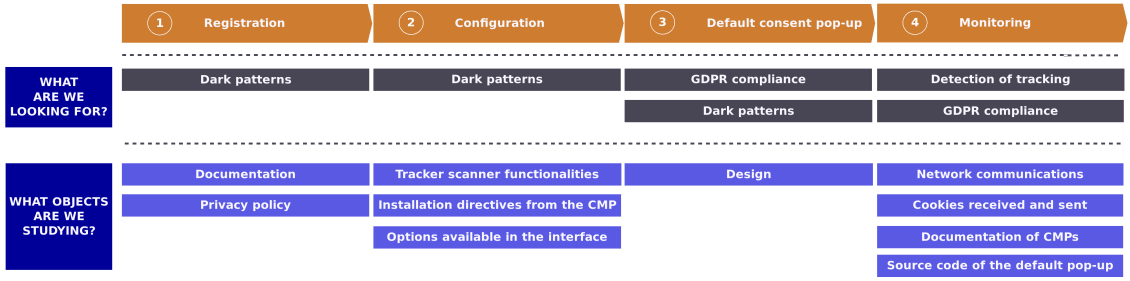


Figure 5.2 – **Study of legally and/or technically problematic design choices.** This flowchart identifies the elements analyzed in this article.

as the implantation of cookies in their terminal, with the same degree of simplicity [41, par. 30 p. 8].

5.3.1 Detecting manipulation by CMPs

To answer the research questions listed in Section 5.1, we built the following experiments. The different parts of our study are summarized in Figure 5.2 and further explained in the rest of this section.

(1) Registration and (2) Configuration processes. In order to evaluate CMPs while minimizing possible interferences, we created one empty website per studied CMP under our EU institution's 2nd level TLD : `cmp-name-version.inrialpes.fr`. For each available consent pop-up version (free, paid, etc. – see Table 5.2) of a studied CMP, we installed one version pop-up per dedicated website hosted on `cmp-name-version.inrialpes.fr`.

When installing a CMP service, we select GDPR-compliant version of consent pop-ups when asked. CookiePro proposes to either set up a consent pop-up directly on their website without creating an account (we call it "unlogged" version) or by creating an account ("logged" version) – in this case, we studied both versions.

When necessary, we distinguish between the *registration* process, which consists for the publisher to fill a form to get access to the CMP services, and the *configuration* process, which consists to configure the consent pop-up according to the needs of the publisher. In each case, we take screenshots during the whole process, matching our observations with known dark patterns [28, 42, 43] and legal requirements from previous works [7]. We list problematic behaviour observed, such as "dark patterns" in both processes, and categorize them from legal and design point of views using previous work definitions (Taxonomies from Gray et al. [28] and Mathur et al. [43], CNIL recommendation [44], list of legal requirements from Santos et al. [7, Table 6]).

(3) Default consent pop-up. For each service that we installed (Table 5.2), we followed the instructions of the CMP and installed the version of the pop-up proposed by CMP *by default*, that is without any modifications in the proposed interface or alternations to the source code of the proposed code snippet to be added to our experiments website (we used one subdomain per CMP service, as explained in the beginning of this section). In each installed consent pop-up, that we now call *default consent pop-up*, we identify potential manipulative strategies in the configuration process as well as potential violations of legal requirements for GDPR-valid consent in the default

CMP	Company location	Service tested	Price	Login required	Subdomain used for tests
CookiePro by OneTrust	UK (London) US (Atlanta)	Free CMP builder	Free	No	cookiepro-free.inrialpes.fr
		Free Account	Free	Yes	cookiepro-free-logged.inrialpes.fr
		Standard Account	$30/mo. ($360/y.)	Yes	cookiepro-paid-1.inrialpes.fr
Quantcast	US (San Francisco)	Choice	Free	Yes	quantcast-free.inrialpes.fr
Cookiebot	DK (Copenhagen)	Free Plan	Free	Yes	cookiebot-free.inrialpes.fr
		Premium Small	9 €/mo. (108 €/y.)	Yes	cookiebot-paid.inrialpes.fr
Crownpeak	US (Denver)	Business	$1,000/y. (Premium)	Yes	crownpeak-paid.inrialpes.fr
Cookie Script	LH (Vilnius)	Free (prev. "Starter")	Free	Yes	cookiescript-free.inrialpes.fr
		Lite	6 €/mo. (72 €/y.)	Yes	cookiescript-paid-1.inrialpes.fr
		Plus	9 €/mo. (108 €/y.)	Yes	cookiescript-paid-2.inrialpes.fr

Table 5.2 – **List of CMPs selected and installed for experiments.** Prices indicated when publicly available on the companies' websites.

consent pop-up obtained.

④ **Monitoring and analysis of the network communications.** To detect tracking cookies and other suspicious behaviors, we rely on the Firefox web developer tools as well as Ernie extension [38], and visit the subdomain `cmp-name-version.inrialpes.fr`, one per each CMP service. We record all HTTP(S) requests and responses, cookies stored/sent that give indications of possible data collection. We open the page in the main and hidden tab of Ernie, a functionality that has the ability to detect shared identifiers. We check the findings of Ernie to display cookies associated with the page load, and detect if these cookies are performing one of the six types of user tracking described by Fouad et al. [39]. We then repeat the experiment, (1) giving a full consent by clicking "Accept all" on the consent pop-up, and (2) refusing to give any consent by clicking "Reject all" on the pop-up (when available). When no "Reject all" button or similar option was provided on the first page of the consent pop-up, we decline consent for all categories in the customization interface. We record our observations, and try to explain them with the help of the documents provided by the companies such as Privacy Policies and commercial documentation. We keep a record of these documents at the date of the consultation. We also search in the code of the consent pop-ups to find possible unnecessary data sent to third-parties.

Additionally, we take the name of each studied company as recorded in the CMP list [45] provided by the IAB Europe, and search for it in the Global Vendor List (GVL) [46] for a possible matching to identify companies that operates both as vendor (advertiser) and CMP. When a company is referenced in both lists, it indicates that it has both (1) an interest into using trackers as a vendor, and (2) the possibility to control the way trackers load on websites as a CMP. This dual position can lead to an ethically questionable situation.

5.3.2 Ethical considerations

Our study was conducted on an empty website hosted by our French institution, and involved real companies registered as CMPs in the IAB Europe TCF Framework. Our study did not involve real users, but instead took the role and simulated the user journey of website publishers when installing services proposed by CMPs.

We installed a consent pop-up directly via a website of a CMP, whenever possible (which is the case of CookiePro Free CMP builder, "Free" account, and "Standard" account, Cookiebot free, Crownpeak Business, and Cookie Script Free, Lite and Plus). However, for TrustArc, and

LiveRamp, we had to contact the companies via contact forms or emails. We intentionally shared our main purpose of the study, which is academic research, in order to provide transparency as to the purpose of the usage of selected CMPs. By doing so, we ensured not to deceive the CMP companies.

However, our experience demonstrates that OneTrust and LiveRamp decline to give us access to their paid services, even when we were ready to pay for their paid versions. We later managed to include CookiePro (by OneTrust) paid service when directly accessible online. TrustArc did not respond to us within one month, thus not allowing us to study their services. It should be noted that TrustArc is the only company to our knowledge that enforces a contractual "Acceptable use" policy preventing any "attempt to discover any source code or underlying ideas or algorithms of the Services" without a written prior agreement.

Open question for the research community. We therefore raise the question whether researchers need to inform the studied services of the purposes of their research or not. As our experience shows, transparency and openness about research goals often implies that only some of the services can be studied.

5.4 Findings

Our goal in this section is to analyze the whole process followed by website publishers when they want to add consent pop-ups to ensure GDPR compliance to their websites. We distinguish in our observations of the configuration process between the misleading nature of the process itself towards the publisher, and the presence of options that may lead publishers to deploy non-compliant consent pop-ups. In the latter case, we also highlight whether these options are active by default, or require an active action by the publisher, as well as the potential presence of any help or advice from the CMP. Therefore, we describe our findings from five different angles guided by our research questions from Section 5.1 :

§5.4.1 The registration process of consent pop-ups via websites of CMPs ;

§5.4.2 Compliance of default consent banners generated by CMPs ;

§5.4.3 The configuration process of the consent pop-ups provided by CMPs ;

§5.4.4 The use of tracking detection tools ("tracker scanners") provided by CMPs and their functionalities ;

§5.4.5 The privileged position of CMPs and their potential collection of data for their own purposes.

5.4.1 Registration of consent pop-ups

In this section, we address the first research question by evaluating the registration process on CMP websites, which is the first step that website publisher performs in order to install a given CMP :

— **RQ1.** Do CMPs use ethically and/or legally problematic strategies known as "dark patterns" in the generation process of their consent pop-ups, to influence the publisher in their own interest ?

Despite this issue being less related to privacy, we think it is important to highlight as it contributes to the discussion regarding the manipulative role of CMPs. For each step of the registration process, we identify the presence of dark patterns aimed at manipulating website publishers and describe it using the terminology of the state-of-the-art works on dark patterns by Bosch et al. [22] and Mathur et al. [43].

Compliance vs. consent rate. First, we observed that several CMPs claimed that their consent pop-ups are "increasing consent rates." We have found one example of such behavior in our study of the Crownpeak CMP. Fig. 5.3 shows a screenshot of the Crownpeak commercial website, where this CMP explicitly states that their pop-ups are "Made for Marketers", while the CMPs of their competitors are instead "Made for Compliance/Privacy".

Fig. 5.4 shows an example from the website of CookiePro, a CMP further studied in our experiments. CookiePro argues that they can "maximize opt-in" and even provide an A/B testing service to compare consent rate between two pop-ups.

	Crownpeak Universal Consent Platform	Other Consent Platforms
Made for Marketers	Yes	No: Made for Compliance/Privacy
Automated list of all third-party profiling on your website	Yes	Limited. Only detects and manages cookie-based technologies
Real-time scanning for all first- and third-party technologies on your site, based on real user sessions	Yes	No

Figure 5.3 – **Crownpeak comparative advertisement "Made for Marketers".** Source : https://www.crownpeak.com/products/privacy-and-consent-management/, screenshot taken on 23 November 2021.

Indeed, the objectives of the services offered by these companies can be divided into two categories, depending on their role. The first, which stems from the obligations imposed by the various data protection laws, consists in assisting publishers in their compliance process with these laws. In particular, this involves guaranteeing the compliance of the collection of user consent. The second, which stems from their for-profit purpose and, sometimes, from their experience as digital marketers or data brokers, is to help publishers maximize their income from personalized advertising. These two roles often have antagonistic characteristics, as users refusal can reduce the volume and/or relevance of the data processed for marketing campaigns, and thus the revenues derived from them. It is in the interest of CMPs to use techniques that keep the rate of user consent high, while ensuring the validity of that consent. There is therefore a conflict of interest here that can lead to the use of deceptive designs to try to propose a product that can satisfy both legal and economical requirements, as explained by Santos et al. [6].

Nudging towards paid or logged-in versions. Some CMPs also encourage publishers to sign up for paid plans by using deceptive design techniques. On their pricing page, CookiePro publishes a comparison table [47] with their most expensive plan labelled as "popular". This dark pattern, called *Pressured Selling* by Mathur et al., is based on "defaults or often high-pressure tactics that steer users into purchasing a more expensive version of a product" [43]. CookiePro's website also

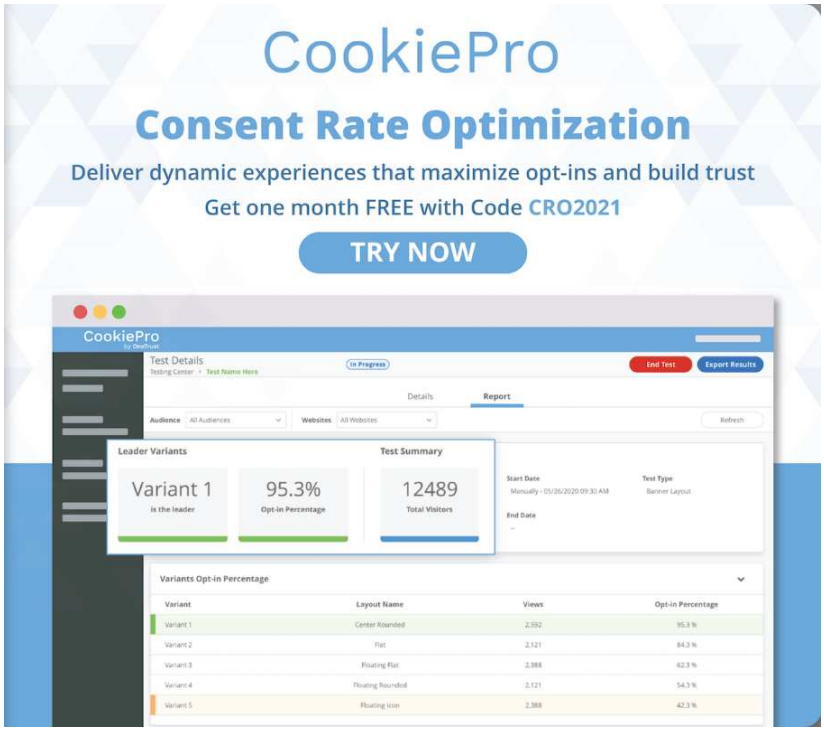


Figure 5.4 – **CookiePro advertisement about "Consent Rate Optimization" with a trial coupon and A/B testing example.** Source : https://app.cookiepro.com/, screenshot taken on 26 November 2021.

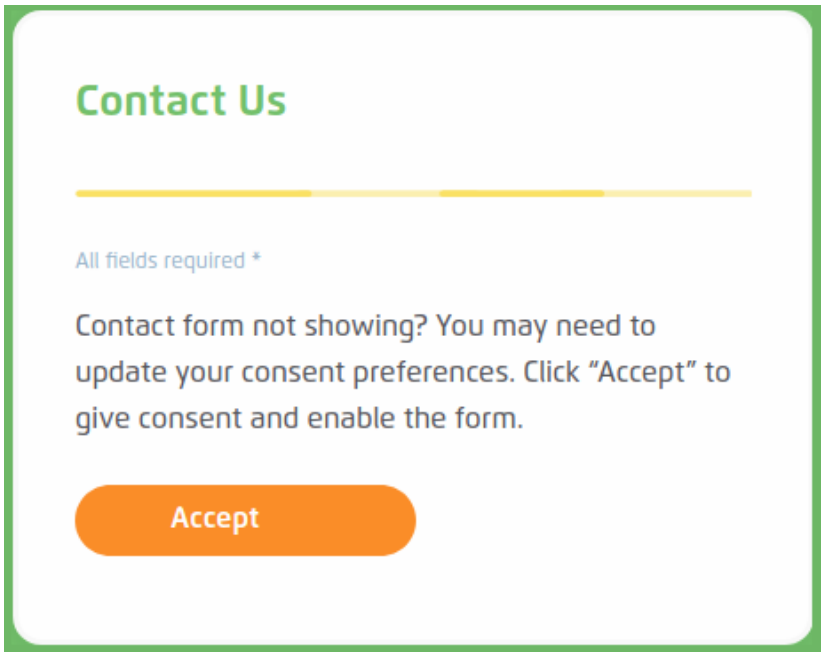


Figure 5.5 – **LiveRamp contact form is not visible without giving a positive consent.** Source : https://liveramp.com/contact/, screenshot taken on 24 November 2021.

shows a chatbot with preselected options which can redirect publishers to paid plans by proposing one month free trial coupons [48].

Finally, all studied CMPs except CookiePro Free CMP builder force the publishers to create an account on their platform to be able to access the service. This practice, labelled as *Forced registration* by Bosch et al. [22], consists of restricting access to certain features to registered and logged-in users, even when it is not necessary to provide the service. In the case of CMPs, while this choice may be justified when managing galaxies of websites with several sub-domains and users of various geographical origins, it may be questionable in the case of simple, entry-level services presented as free.

Potential violation of 'specific" consent. When installing Quantcast and filling the contact form on their website [49] with a EU-based country name, the form displays a checkbox with the following statement :

> *"I wish to receive future informational and marketing communications from Quantcast, and I understand and agree to the privacy policy."*

Selecting this checkbox is not mandatory to validate the installation process of Quantcast, however the phrasing is misleading since the user has to agree to receive marketing communications and agree to the privacy policy at the same time. Using a single checkbox for the acceptance of the privacy policy, which is generally mandatory to use a service, and for the subscription to a newsletter, which is optional and requires to consent, may nudge the user toward checking the box, thinking that it is impossible to finalize the request otherwise. From legal perspective, such design raises a potential violation of a legal requirement for *specific consent* that requires separate consent per each specific purpose [3, Art.4(11),6(1)(a)], as described recently by Santos et al. [7, Sec. 5.3].

We studied the registration process of LiveRamp CMP, that is however not included in the further analysis due to lack of installation (see Table 5.1). When the website publisher tries to access the CMP or create an account on their website, the publisher is presented with a consent pop-up with both "Accept" and "Deny all" options. However, if the visitor decides to deny all processing in the consent pop-up, the contact form [50] is not displayed. Instead, the form is replaced by a message asking for "update [of] consent preferences", as displayed in Figure 5.5. If the visitor selects the "Accept" option, the contact form displayed but it does not include any option to refuse subscription to automated prospection. After filling the form, the company sends on average two emails per week to the address used to contact them, all seeming to come from the same LiveRamp employee. Since the publisher cannot access the CMP service, create an account, or send a contact message without allowing the CMP to reuse their data for other purposes, this practice constitutes a *tracking wall* design strategy that potentially violates the requirement of *free consent* [3], as explained in 2020 by Santos et al. [7, Sec. 5.2].

5.4.2 Consent pop-up with default options and its compliance

In this section we study the compliance of the consent pop-ups proposed by various CMPs "by default". To obtain such "default" pop-up and install it on our experimental website, we follow the default options provided by the CMP without any modifications. We then study the following research question :

— **RQ2.** Is a consent pop-up generated with the default options provided by the CMP compliant with EU legal requirements ?

We analyzed the ten default consent pop-ups generated by CMPs, and mapped our observations with one most discussed requirement for valid consent from Santos et al. [7, Table 7], called *Balanced choice*. Our goal was not to make an exhaustive evaluation of all consent pop-ups with relation to the 22 requirements listed in this work, but instead to focus on the most critical and important requirement instead. We also detect several practical issues around inclusion of advertising vendors and non-possibility to object to legitimate interest legal basis in the rest of this section.

Compliance on requirement for *Balanced choice*. Several DPAs have stated that users wishing to express their refusal should not encounter a disproportionate obstacle. For example, in the last version of their Guidelines on consent, the French DPA highlight that rejection should present the same level of simplicity that the one of acceptance [51, Art. 2(30)]. Santos et al. call this requirement *Balanced choice*, and give the following interpretation from Art. 7(3) of the GDPR and from publications of DPAs [7, Table 7] :

> *"From Article 7(4) of the GDPR which states that withdrawing consent should be as easy as giving it, we additionally interpret that the choice between "accept" and "reject" [browser-based tracking technologies] must be consequently balanced (or equitable)."*

We found out that six out of ten studied consent pop-ups – Quantcast, Cookiebot free, Cookiebot paid, and Cookie Script Free, Lite, and Plus – showed a difference between the "Accept" and "Reject" button by default, making the "Accept" choice more salient. CookiePro "logged" did not display the "Reject" button by default. Only the "unlogged" version of CookiePro shows in the first layer of its default banner both buttons with the same font, color, and size. However, the second layer of this service places "Allow All" on top of the page, while "Reject All" and "Confirm My Choices" on the bottom, making it hard for end users to reject or customize their preferences (see Fig. 5.6).

We therefore conclude that almost none of the studied services provide full compliance with the *Balanced choice* requirement and hence are introducing a violation to the *unambiguous consent* requirement [3, Art. 4(11)] and to a requirement that withdrawing consent should be as easy as giving it [3, Art.7(4)].

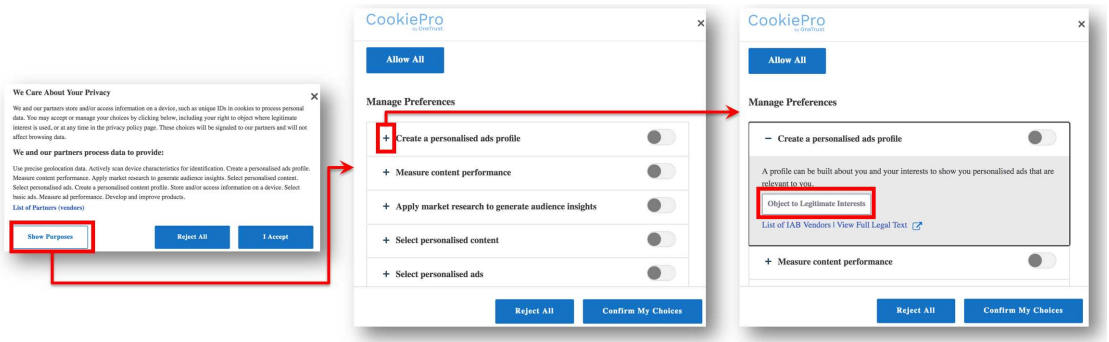


Figure 5.6 – **CookiePro Free CMP builder "unlogged" consent pop-up.** Objection to Legitimate Interest is becoming visible only after clicking on the "+" button in the 2^{nd} layer of the consent pop-up interface. Screenshot taken on our experimental domain on 22 November 2021.

High number of vendors included by default. In Quantcast Choice, the management of vendors (partners) by the website publisher is made via a different tab of the CMP configuration interface. By default, the whole IAB Europe Global Vendors List is included, representing 751 companies as of 28 May 2021. Publishers can manually revoke them on an opt-out basis. Publishers can add the Google Ad Tech Providers (ATP) list, containing a total of 641 companies at the same date, and also add their own partners with a link to their privacy policy. The complete process is designed to make the inclusion of vendors easy (large number of vendors included by default, addition of Google vendors in one click) while blocking vendors needs to be done manually.

In the "Free CMP Builder" service offered by CookiePro, it is not even possible to customize the list of vendors at all. In the "logged" version of CookiePro free (used with an account), the CMP built by default a consent pop-up with an "Accept" button and no "Reject" on the first page, and an "Allow all" button on the top of the second page. Both lead to a bulk consent and close the pop-up.

On the opposite, Crownpeak Business (a "Premium" service), Cookiebot, CookiePro Standard, and Cookie Script include only the vendors that were found on the website when scanning it, or that were added manually by the publisher.

Delayed update of the vendor's list in the consent pop-up. After the initial configuration of the banner and its installation on the website, a publisher can still include additional trackers. Technically, this action by itself cannot trigger an immediate update of the vendor's list presented to the visitors in the consent pop-up. Depending on the service offered by the CMP, the publisher should either 1) manually add the tracker to the consent pop-up, 2) trigger a manual scan of the website, or 3) wait for the next automatic scan to occur. The first technique implies that a publisher has sufficient technical and legal knowledge of the ecosystem, which is not obvious. The second one is not always available, can have specific limitations (e.g., one scan per day for Cookie Script). The third one is only proposed at large time span (unless the publisher subscribes to additional fees with Cookiebot). Moreover the two first techniques require publishers to take an additional active action, which is unlikely for the least informed ones. This situation can lead to issues such as outdated and incomplete consent pop-ups remaining on websites for several weeks after the addition of new trackers, in violation of the legal requirements for valid consent.

Manipulative behaviour restricting objection to legitimate interest-based processing. According to the GDPR, processing of personal data can be performed lawfully only if one of the six *legal basis* of processing applies [3, Article 6(1)] : while the most known legal basis is *consent*, some advertisers rely on the other legal basis, called *legitimate interest*. The rules around application of this legal basis in practice are complex and understudied in the scope of Web applications. In this work, we raise our observations regarding the user interface of the consent pop-ups proposed by default and integration of *legitimate interest* legal basis. Even when the default consent pop-up is compliant with the legal requirements for consent, it can still contain manipulative strategies against the users' right to object to data processing based on the legal basis of *legitimate interest* [3, Art.21].

Fig. 5.6 shows the free "unlogged" version of CookiePro, where the buttons for objecting legitimate interest-based processing are not visible by default, and the user needs to click on purposes to see them.

Quantcast consent pop-up also contains a problematic design by default. It includes the following text :

> *"With your permission we and our partners may use precise geolocation data and identification through device scanning. You may click to consent to our and our partners' processing as described above. Alternatively you may click to refuse to consent or access more detailed information and change your preferences before consenting. Please note that some processing of your personal data may not require your consent, but you have a right to object to such processing."*

This text does not indicate explicitly that a user who clicks on the "Disagree" button is only refusing to give an explicit consent to the processing based on it, but is not objecting to other processing, based on the legal basis of *legitimate interest*. To completely refuse any processing of her data, the user who wants to object should instead select *More options*, *Legitimate Interest*, and then object to several or all vendors. Therefore, users do not have information by default on how to object to legitimate interest-based processing in the Quantcast consent pop-up.

5.4.3 Configuration options leading to the deployment of manipulative and/or non-compliant consent pop-ups

In this section, we analyze the options offered by CMPs to configure their consent pop-ups, and we list the ones that can can nudge publishers towards deploying manipulative and/or non-compliant consent pop-ups. We respond to the following research question in this section :

— **RQ3.** Do the default configuration options of consent pop-ups encourage publishers to comply with the requirements for collecting legally valid consent ?

Option to create consent wall with reduced service. The Quantcast configuration interface includes a field to add a "Non-consent redirect URL". This option can be used to set up a *consent wall* and *reduced service*, two design strategies described by Gray et al. [24].

A *consent wall* is designed to "block access to the website until the user express their choice regarding consent. This design choice allows a user to select between acceptance and refusal ; however, the concrete use of the website is blocked until a choice has been made.". While it is an open question whether *consent wall* violates the EU law [52], Gray et al. [24] argue that "such as blocking access to a website until a user expresses a choice — will force the user to consent and therefore it possibly violates a *freely given* consent", referring to the Article 7(4) and Recital 43 of the GDPR [3]. This design strategy is also criticized for introducing *obstruction* "in placing visual and interactive barriers between the target of the user's interaction" and the consent pop-up.

Reduced service is a consequence of a choice made by the user in the consent pop-up interface and means "the practice of a website offering reduced functionality – for example, allowing a user access to only limited number of pages on a website – based on their consent configuration options." From a legal perspective, Gray et al. [24] argued that such design strategy could be legally compliant only if "it clearly enables the user to choose between various options of access".

When Quantcast provides the options of *consent wall* and *reduced service* in its consent pop-up configuration, it also provides the following documentation [53] :

> *"Use this if you would like to send a user to an advertising-free version of your site, a minimized content experience, or to a page that explains why consent is important for specific features to function on your site."*

Based on the prior work [24], this configuration option can lead to a potential violation of the requirement for *freely given consent* [3, Art.7(4)]. Moreover, if the website publisher does not provide reject option, then such practice may constitute *tracking wall* (a consent wall that gives

only one option : to consent and accept any terms offered by the website) recognized as unlawful by the majority of regulators and Data Protection Authorities in the EU [24, Sec. 4.1].

5.4.4 Problems in the configuration process involving a tracker scanner

In this section we study the "tracker scanner" functionality provided by CMPs. Tracker scanner allows website publishers to automatically detect trackers on their websites, and sometimes even to evaluate the overall compliance of their websites. Some scanners even propose automatic updates to the consent pop-up interface, taking into account the detected trackers and their purposes. While it is a very complex task to evaluate effectiveness of tracker scanners at scale because (1) such scanner tools are not open-sourced ; (2) there is a lack of testing websites with all potential trackers integrated.

Therefore, we analyse the tracker scanner service provided by the CMPs on our empty website. An *honest scanner* should detect no tracking since our website does not contain any content. With this experiment, we aim at answering the following research question :

— **RQ4.** What are the functionalities and the impacts of tracker scanners provided by CMPs, regarding legal compliance, role of CMPs, and publishers behaviour ?

We found out that four CMPs — CookiePro, Cookiebot, Crownpeak, and Cookie Script — propose tracker scanners. These scanners show notable differences regarding both their appearance and functionalities. The main observations are summarized in Table 5.3.

CMP	Service	Needs account	Gives report	Gives advices	Auto. updates purposes in pop-up	Auto. updates vendors in pop-up	Auto. updates cookie/privacy policy
CookiePro	Free unlogged	No (*)	✓	✓	×	×	×
	Free account	Yes	✓	✓	✓	✓	✓
	Standard account	Yes	✓	✓	✓	✓	✓
Cookiebot	Free	No (**)	✓	×	✓	✓	×
	Paid	Yes	✓	×	✓	✓	✓
Crownpeak	Business	Yes	×	×	✓	✓	×
Cookie Script	Free	No	✓	×	✓	✓	×
	Lite	Yes	✓	×	✓	✓	✓
	Plus	Yes	✓	×	✓	✓	✓

Table 5.3 – **Comparison table of tracker scanners' functionalities. (*) Name and email required (**) Email required but not stored**

Scanners providing only a basic report. The CookieBot scanner allows to create a free account, but the scanning functionality is then limited to five pages per website. It sends the scan report as a HTML file by email. The information given is short and basic : date, domain name, server location, number of cookies found, detailed list by category (e.g. "Necessary"). The detailed view of a cookie contains only basic information : cookie name, provider, purpose (e.g. "Stores the user's cookie consent state for the current domain"), initiator (e.g. "Script tag"), destination of data, and evaluation of the adequacy of the international data transfer under the GDPR. The report does not provide detailed information about the vendors, nor does it make any suggestion for actions. Strangely, we noticed that the cookie for storing consent registered by CookieBot is included in the scanner report (and categorized as *Necessary*), even if we tested an empty website without any pop-up – CookieBot automatically assumes that we will install their pop-up on our website.

Scanners inciting publishers to subscribe to paid plans. The CookiePro unlogged scanner is proposed directly from the home page of the CMP [48]. The categorization is made by matching the cookies found with the Cookiepedia database (also owned by OneTrust). In order to perform an analysis, the publisher needs to fill a form with a name, an email address, and the URL of the website to scan. CookiePro scanner displays an overview of its finding in the browser, and sends the report by email as a PDF file. The first overview contains four sections : (1) a summary of the website, with the number of pages and the number of cookies found, (2) a *Privacy checklist* which indicates if the scanner was able to find a consent pop-up, cookie policy, and privacy policy, (3) a suggestion of paid plans and options, and (4) a detailed list of the cookies found (when applicable). The CookiePro's detailed PDF report contains the number and list of cookies, tags, forms, and webpages found, analyzed and sorted by categories such as first/third party, session/persistent, web object types, and cookie purposes. It also includes an analysis of the CMP with "Recommended actions".

Nevertheless, and despite our webpage being absolutely empty (no cookie, script, tag, or form), the CookiePro scanner still labels our empty website as *"High Risk"* because it doesn't find any privacy or cookie notice, nor any consent pop-up. It appears that the scanner tool *is not able to adapt to a website without cookies or other trackers* ! The scanner makes scary misleading statements such as *''Our scan reveals a particularly high risk with respect to with European ePrivacy Laws, which have requirements for transparency and consent related to the types of cookies you have on your site."*. In consequence, the scanner is nudging the website publisher to "contact legal advice" and "scan [our] site on a regular basis".

With the free version of Cookiebot, the drop-down list titled "scanning frequency" is present but is disabled (greyed). Only the default frequency (monthly scan) is visible. On the premium version of the same service, the list is activated, and the scanning frequency can be changed from monthly to daily, however this change is charged an additional 62 € per month. Since the box is visible to publishers in the free version of the CMP, but the price of the additional feature is not visible until they have access to the premium version, this can lead publishers to subscribe to the premium plan first, thinking they will have access to highest levels of scan frequencies, and then to subscribe to the additional feature when they realize it is not included. This form of dark pattern is known as *Hidden Costs* [28, 42, 43].

CookiePro often provides "Free trial coupons" on their website and via their commercial emails. However, using this coupon for subscription requires providing credit card details, and giving authorization to the CMP to *"automatically charge this payment method whenever a subscription is associated with it"*. This dark pattern has been identified by Brignull as *Forced continuity* [42].

Delayed scan results. Finally, with Cookie Script, the scan is triggered by default when configuring the consent pop-up, and before the installation of the pop-up on the website. However, the scan report is displayed only some minutes later, and does not include the cookie set by the CMP itself, nor informs about its presence. In consequence, if the publisher does not launch a manual scan, they could install the consent pop-up without knowing anything about this cookie before the next automatic scheduled scan, which will happen one month later. However, nothing indicates that it has any tracking role. After scanning a website, the tool redirects to a report page prompting to *"Add cookie compliance"* with an exclamation mark, even if no cookie was detected on our empty website. Since our website does not include trackers, the usage of a consent pop-up is not mandatory and such solicitation, like in case of CookiePro, is not needed. Cookie Script also adds

a link to the report in the consent pop-up, introducing confusion to the website visitors who might believe that the visited (empty) website contains trackers.

Regarding the detection process, we can therefore conclude that CookiePro and Cookie Script are not mentioning the presence of any cookie on our empty website, while Cookiebot mention its own consent cookie, assuming that we will install their banner.

5.4.5 CMP abusing its position to collect data for its own use

In this section we monitor the resulting empty web site (one per CMP service, as described in Table 5.2) that includes the CMP consent pop-up. Our goal is to assess if this integrated consent pop-up content could be leveraged to collect data for the CMP own use, and whether some CMPs exploit their privileged position to actually collect data for their own use. We therefore aim at answering the following research question :

— **RQ5.** Are CMPs abusing their central and privileged position and their presence on a large number of websites to collect data for their own use ?

Case of Quantcast Choice. When a page including *Quantcast universal tag*, the Javascript code provided by Quantcast to provide Quantcast Choice CMP, is loaded by a browser, it sends 10 distinct third-party requests, aiming to 6 different subdomains. At the time of our first tests in April 2021, the requests to `edge.quantserve.com`, `pixel.quantserve.com` and `rules.quantcount.com` were even insecure (HTTP), despite the website being accessed in HTTPS. These different requests load content in the form of Javascript code hosted on CMP's managed domains. The most important part is the `choice.js` script, which controls the display of the consent pop-up and loads other parts.

We first tested the Quantcast Choice service in January 2021 : this service loads the `choice.js` script that further sends a request to `pixel.quantserve.com` to fetch a 1x1 gif image. Upon loading this image, `pixel.quantserve.com` sets a third-party cookie named `mc` with a random value, that is different across our session and private Firefox container, indicating that such cookie is *user-specific* (see the details of detection of such cookies in the description of Ernie extension we used for these experiments [38]). This cookie have an expiry time of one year. Notice that this tracking pixel was integrated *by default* in all Quantcast Choice banners *even before the user makes a decision regarding acceptance or refusal of consent in the pop-up interface* ! This finding confirms the behaviour reported by Santos et al. [6]. The requests to these Quantcast servers are also flagged as tracking by tracking filter lists such as Disconnect [*].

After an update on March 5th, 2021, the behaviour of the `choice.js` script has changed : the request for 1x1 invisible pixel to `pixel.quantcount.com` does not set a tracking cookie anymore *unless the user gives a positive consent*, If the user does not consent, no `mc` cookie is set in the browser. If this new behavior fixes a major compliance issue (that is, tracking before consent), it also demonstrates the ability of CMPs to include content unrelated to consent management at any time, and without informing nor giving the publisher a possibility to oppose.

Notice that the Quantcast Choice today includes the tracking cookie (after user's consent) on an otherwise empty website without properly informing the website publisher. We have found only one possible explanation for the presence of this tracking technique in the consent pop-up : Quantcast merged the "Count and Measure" services in the "Universal Tag", as explained in Quantcast documentation [54] :

*. https://github.com/disconnectme/disconnect-tracking-protection/blob/21134d05e7a407739d7db0b695cbbf359afffdd2/services.json#L5646

> *"The Universal Tag includes both Quantcast Choice & Quantcast Measure, our audience insights and analytics tool. This enables us to provide Quantcast Choice for free to all users and makes implementation of the combined tag easier."*

To conclude, even if it is possible that the `mc` cookie attached to the request made to `pixel.quantserve.com` is a part of Quantcast measure service, the CMP does not disclose any other information about this cookie in its privacy policy [55].

Case of Cookie Script free. With Cookie Script free, the banner itself does not include any tracking request. However, it does include a link to the page of the last scan report ran on the website, previously described in Section 5.4.4. The tracker scan page includes a *Google Analytics* service, as well as social sharing buttons, all of which generating a total of 41 third-party requests and the deposit of 6 cookies without the user's prior consent according to Firefox developer tools. 16 of these requests are flagged as related to "known trackers" in the Disconnect list. Details are listed in Table 5, Appendix A.1.

5.5 Discussion

5.5.1 Main outcomes

CMP	Service	Consent optimisation	Incit. to pay	Unspecific cons.	Unbalanced choice	Include all vendors	Delayed list update	Restrict objection	Redirect option	Tracking
Related sections		4.1	4.1/4.4	4.1	4.2	4.2	4.2	4.2	4.3	4.5
CookiePro by OneTrust	Free CMP builder					×				
	Free Account	×	×			×				
	Standard Account	×	×							
Quantcast	Choice			×	×	×		×	×	×
Cookiebot	Free				×					
	Premium Small				×					
Crownpeak	Business	×								
Cookie Script	Free		×		×		×			
	Lite		×		×		×			
	Plus		×		×		×			

Table 5.4 – **Summary of issues found in tested services.** Identified problems are marked with × .

In this section we discuss our findings (summarized in Table 5.4) and the situation in general.

Related work has shown that end-users are highly susceptible to manipulation by dark patterns [21,43]. They also showed the important role that CMPs have, at the crossroads of the digital advertising ecosystem [6]. Our work goes further by analysing the whole consent pop-up system, including the relationships between CMPs and website publishers. In a context where law and technology are rapidly evolving, these CMPs are trying to position themselves as privacy compliance experts. However, the reality is much more subtle.

First of all, we observed that CMPs often do not help improving user's privacy when visiting a website. On the one hand, *user consent is often wide, non-informed, and subject to manipulation.* More precisely, Quantcast and CookiePro tend to propose to the publishers by default the entire Global Vendors List provided by the IAB Europe, which contained 751 companies end

of May 2021, potentially complemented with the Google Ad Tech Providers (ATP) list that is almost the same size. In their turn, the publishers, in particular when they rely on default settings, present the same list to the users, with several hundreds of companies. So if a user agrees, she explicitly accepts her personal data to be exchanged among hundreds of companies, instead of being limited to those present on the visited website. Then a user cannot comprehend such a long list, and Veale and Borgesius [56] have demonstrated that the "informed choice" requirement cannot be fully met in these circumstances, which theoretically voids the user consent. On the opposite, by default, the services of Cookiebot, Crownpeak, and Cookie Script do not include the whole list of vendors but instead customize it automatically by using the results of a scan, which clearly benefits to the end user.

In addition, many CMPs present themselves as being able to help publishers increase the consent rate of their web site visitors, which raises questions about the very function of consent pop-ups. Indeed, it implicitly validates that the purpose of these pop-ups is ultimately more about "extracting" positive consent than letting users make a free and informed choice.

On the other hand, *CMPs consent pop-ups can create additional privacy and security issues.* Our methodology involves creating an empty website that does not include any tracking tool. However, by adding a consent pop-up, we found analytics tools – presented as meant to provide statistics on consent rates – in Quantcast, and in a scan report page made available by Cookie Script – presented as meant to monitor views of the scan report page. This finding indicates that CMPs may actively participate in the overall rise of user tracking on the web. Then, the addition of a consent pop-up in a web site requires dynamically loading third-party scripts, which mechanically gives a lot of power to the CMPs as owner of the scripts. For instance, the CMP may add or remove a tracking tool at its own discretion (as we observed with Quantcast), and it is not clear whether the publisher would be either informed or able to refuse. The system could also be diverted by an attacker who may add a malicious script in the publisher's website. This situation raises privacy and security risks.

Secondly, CMPs themselves often use deceptive design schemes towards publishers, to entice them to subscribe to their paid plans. This happens even when the publishers do not include tracking content on their websites, and therefore do not formally require to include a consent pop-up. For example, the tracker scanner result can include messages such as "High Risk" CookiePro or "Add Compliance" CookieScript when it does not find a consent pop-up or privacy policy, sometimes even on a systematic basis. The CMPs also use iconography and color-code to play on the fear of non-compliance. Of course, a possible explanation for this behavior may come from their (presupposed) business model. They are private, for profit companies, whose existence directly depends on their ability to convince their clients, the publishers, of the need to subscribe to their paid offers. They may also be themselves linked to advertising/marketing groups (e.g., Quantcast), or data brokers (e.g., LiveRamp, new name of Acxiom Corporation, after purchasing the LiveRamp company).

Thirdly, CMPs should probably be considered as data controllers. The present work reinforces the findings of Santos et al. [6] by providing additional arguments to qualify CMPs as data controllers. For instance, this becomes obvious when considering a CMP manipulating the website publisher during various steps in the configuration process, or by recommending the publisher to include a consent pop-up in an empty website where it could be omitted, or by generating non compliant default consent pop-ups.

5.5.2 Recommendations

Despite the fact that CMPs are positioning themselves as compliance specialists, website publishers should keep a critical eye on the consent collection process. Indeed, they remain data controllers under the GDPR.

Regulators also have a major role. They can provide guidelines and recommendations to highlight good practices, as did the CNIL French DPA in [40, 41, 44]. They can illustrate them with examples of "do and don't" designs [57], and help publishers and CMPs to implement infrastructures to manage user choices that follow state-of-the-art legal and ethical recommendations.

5.5.3 Consent pop-ups beyond third-party cookie era

On their websites, several CMPs (OneTrust, Quantcast, LiveRamp) insist on the importance of preparing for the post third-party cookie era. This is a consequence of the use of blocking tools by end users, and the fact third-party cookies are increasingly blocked by default by web browsers (Apple/Safari in 2017, Mozilla/Firefox in 2019, potentially Google/Chrome in 2024). Consequently, "Cookie banners" have evolved to more generic "consent pop-ups" meant to inform users and collect their consent, regardless of the tracking technique in use.

CMPs and Ad Tech companies are working on alternatives : some of them already rely on CNAME cloaking ([58] explains that 9.98% of the top 10,000 websites rely on it in 2021); others (e.g., OneTrust, LiveRamp, Quantcast, Google) develop such alternatives as Server Side Tagging, Single Sign-On, or persistent identification [59–62]. IP-based tracking [63] and fingerprinting scripts [64] can also be used with first-party cookies to target non registered users who block or delete cookies. In their February 2021 report [59], the IAB Europe explores "Identity solutions" such as email-based Customer Relationship Management.

Such data is then aggregated in large databases, in a pseudonymized manner, often after hashing the user email address [59, 65]. Of course, this pseudonymization approach enables persistent, cross-device, and cross-site tracking, to the benefit of data brokers such as LiveRamp and their partners [65].

From a privacy viewpoint, in the long run, end users may lose visibility and have less control with this evolution, because an increasing part of the tracking process will happen directly on server side, and it is no longer a matter of storing or removing a cookie in the user's web browser, which is easily viewable. In any case, consent pop-ups are still legally required, the proof of valid consent being needed regardless of the tracking technique in use as reminded by the French DPA in [66].

5.6 Conclusion

In our work, we systematically studied the installation and configuration process of consent pop-ups and their potential effects on the decision making of the website publishers. We made an in-depth analysis of the configuration process from ten services provided by five popular CMP companies and identify common deceptive strategies employed.

By analysing CMP services on an empty experimental website, we identified manipulation of website publishers towards subscription to the CMPs paid plans and then detected that default consent pop-ups often violate the law. We have also shown that configuration options may lead to non-compliance, while tracking scanners offered by CMPs manipulate publishers. Finally, we

identified a CMP that abuses its position to include an additional pixel, flagged as tracker, to the consent pop-up.

Our findings demonstrate the importance of CMPs and we raise concerns around the privileged position of CMPs and their manipulative strategies versus website publishers. Finally, we open a discussion for regulators and policy makers to analyse the behavior, incentives and manipulative strategies of CMPs that affect thousands of websites and millions of end users via the design and configuration options proposed to the publishers.

Acknowledgments

This work was supported by the ANR JCJC project PrivaWeb (ANR-18-CE39-0008) and the H2020 SPARTA Cybersecurity Competence Network project.

We would like to thank the reviewers for their helpful comments, Vera Wesselkamp for her assistance with the ERNIE extension, Jean-François Scariot for his technical support, Cristiana Santos for providing useful legal resources, and Midas Nouwens for his help regarding the analysis of CMPs' plans.

A Appendix

A.1 HTTPS requests in the Cookie Script Free scanning report

Table 5 lists the HTTPS requests observed when visiting the Cookie Script scanning report website by following the link present in the consent pop-up. See Section 5.4.5 for the associated discussion.

#	Domain	File	Initiator	Tracker
1	cookie-script.com	css-99b62-55873.css	stylesheet	
2	cookie-script.com	cookie.svg	img	
3	cookie-script.com	css-b3740-22058.css	stylesheet	
4	cookie-script.com	text.svg	img	
5	static.mailerlite.com	webforms.min.js ?v4a60e9ef938a7fa0240ac9ba567062cb	script	
6	cookie-script.com	js-cF177-34068.js	script	
7	cookie-script.com	helpscout.js	script	
8	cookie-script.com	css-079a7-66634.css	stylesheet	
9	www.googletagmanager.com	gtm.js ?id=GTM-WZXWWWM	cookie-report :31 (script)	
10	static.mailerlite.com	ml_jQuery.inputmask.bundle.minjs ?v3.3.1	webforms.min.js :1 (script)	
11	cookie-script.com	fb.svg	img	
12	cookie-script.com	tw.svg	img	
13	cookie-script.com	ig.svg	img	
14	cookie-script.com	footerarrow.svg	img	
15	cookie-script.com	fontawesome-webfont.woff2 ?v=4.6.3	font	
16	cookie-script.com	favicon.ico	img	
17	**platform-api.sharethis.com**	**sharethis.js**	**script**	**Yes**
18	cookie-script.com	apple-touch-icon.png	FaviconLoader.jsm :191 (img)	
19	cookie-script.com	favicon-16x16.png	FaviconLoader.jsm :191 (img)	
20	cookie-script.com	en.svg	js-cf177-34068.js :30 (lazy-img)	
21	**l.sharethis.com**	**pview ?event=pview&hostname=cookie-script.com&location=/cookie-report &product=inline-share-buttons&url= https ://cookie-script.com/cookie-report ?identifier=Fa78 1 fc6540325F7b8c6bc93**	**sharethis.js :3297 (xhr)**	**Yes**
22	**www.google-analytics.com**	**analytics.js**	**gtmjs :36 (script)**	**Yes**
23	**buttons-config.sharethis.com**	**5e106537dd527900136b1728.js**	**sharethis.js :669 (script)**	**Yes**
24	**www.google-analytics.com**	**collect ?v=1&_v=j96&a=1755241340&t=pageview &_s=1&dl=https ://cookie-script.com/cookie-report ?identifier=Fa7811fc6540325F7b8cébc93b5a7 d9dc&ul=en-us&de=UTF-8&dt=Cookie report fc**	**analytics.js :44 (xhr)**	**Yes**
25	**platform-cdn.sharethis.com**	**skype.svg**	**sharethis.js :4501 (img)**	**Yes**
26	**platform-cdn.sharethis.com**	**facebook.svg**	**sharethis.js :4501 (img)**	**Yes**
27	**platform-cdn.sharethis.com**	**twitter.svg**	**sharethis.js :4501 (img)**	**Yes**
28	**platform-cdn.sharethis.com**	**pinterest.svg**	**sharethis.js :4501 (img)**	**Yes**
29	**platform-cdn.sharethis.com**	**whatsapp.svg**	**sharethis.js :4501 (img)**	**Yes**
30	**platform-cdn.sharethis.com**	**email.svg**	**sharethis.js :4501 (img)**	**Yes**
31	**platform-cdn.sharethis.com**	**messenger.svg**	**sharethis.js :4501 (img)**	**Yes**
32	**platform-cdn.sharethis.com**	**print.svg**	**sharethis.js :4501 (img)**	**Yes**
33	**platform-cdn.sharethis.com**	**gmail.svg**	**sharethis.js :4501 (img)**	**Yes**
34	**platform-cdn.sharethis.com**	**reddit.svg**	**sharethis.js :4501 (img)**	**Yes**
35	**platform-cdn.sharethis.com**	**linkedin.svg**	**sharethis.js :4501 (img)**	**Yes**
36	beacon-v2.helpscout.net	/	helpscout.js :5 (script)	
37	beacon-v2.helpscout.net	vendor.571a2921.js	1 :1 (script)	
38	beacon-v2.helpscout.net	main.c78fc066.js	1 :1 (script)	
39	d3hb14vkzrxvla.cloudfront.net	18437cb5-f086-491c-bd0d-4bcaze2c64b6	xhr	
40	d3hb14vkzrxvla.cloudfront.net	18437cb5-f086-491c-bd0d-4bcaze2c64b6	vendor.571a2921.js :1 (xhr)	
41	beacon-v2.helpscout.net	container-frame.f24f42a4.chunk.js	vendor.571a2921 js :1 (script)	

Table 5 – **List of HTTPS requests observed in the tracking report accessible from the Cookie Script Free consent pop-up. This report is stored on the CMP's website, not in the consent pop-up itself.**

Bibliography

[1] The European Parliament and the Council of the European Union, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," 2002, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058, accessed 29 March 2021.

[2] "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136, accessed on 20 Apr 2021.

[3] "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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679.

[4] 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," *Network and Distributed Systems Security Symposium*, 2019.

[5] 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," in *IEEE Symposium on Security and Privacy*, 2020, pp. 791–809.

[6] C. Santos, M. Nouwens, M. Toth, N. Bielova, and V. Roca, "Consent management platforms under the GDPR : processors and/or controllers ?" in *Annual Privacy Forum (APF'21)*, vol. 12703, 2021, pp. 47–69.

[7] C. Santos, N. Bielova, and C. Matte, "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*, pp. 91–135, 2020. [Online]. Available : https://doi.org/10.26116/techreg.2020.009

[8] "Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH," 2019, http://curia.europa.eu/juris/documents.jsf?num=C-673/17.

[9] "AP : veel websites vragen op onjuiste wijze toestemming voor plaatsen tracking cookies," 2019, gDPRHub : https://gdprhub.eu/index.php?title=AP_-_Consent_to_place_cookies, original source (in NL) : https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies, accessed on 30 May 2021.

[10] "Procedimiento No : PS/00264/2020, RESOLUCION DE PROCEDIMIENTO SANCIONADOR." 2021, gDPRHub : https://gdprhub.eu/index.php?title=AEPD_-_PS/00264/2020, original source (in ES) : https://www.aepd.es/es/documento/ps-00264-2020.pdf, accessed on 30 May 2021.

[11] "Datatilsynet - 2020-31-3354," 2020, gDPRHub : https://gdprhub.eu/index.php?title=Datatilsynet_-_2020-31-3354, original source (in DA) : https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/nov/ugyldigt-samtykke-paa-hjemmeside, accessed on 30 May 2021.

[12] Commission Nationale Informatique et Libertés (CNIL), "Cookies : GOOGLE fined 150 million euros," 2021, https://www.cnil.fr/en/cookies-google-fined-150-million-euros.

[13] ——, "Cookies : FACEBOOK IRELAND LIMITED fined 60 million euros," 2021, https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros.

[14] ——, "Cookies : penalty of 50,000 euros against SOCIETE DU FIGARO," 2021, https://www.cnil.fr/en/cookies-penalty-50000-euros-against-societe-du-figaro.

[15] ——, "Cookies : financial penalty of 35 million euros imposed on the company AMAZON EUROPE CORE," 2020, https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core.

[16] "Cookies equally easily accepted or refused : CNIL orders 20 organisations to comply," 2021, https://www.cnil.fr/en/cookies-equally-easily-accepted-or-refused-cnil-orders-20-organisations-comply.

[17] M. Hils, D. W. Woods, and R. Böhme, "Measuring the emergence of consent management on the web," in *Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 317–332.

[18] 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 *CHI*, 2020.

[19] C. Matte, C. Santos, and N. Bielova, "Purposes in IAB Europe's TCF : which legal basis and how are they used by advertisers ?" in *Annual Privacy Forum, APF*, ser. Lecture Notes in Computer Science, 2020, https://hal.inria.fr/hal-02566891.

[20] IAB Europe, "IAB Website," https://iabeurope.eu/transparency-consent-framework/, accessed on 20 Apr 2021.

[21] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed Consent : Studying GDPR Consent Notices in the Field," in *ACM Conference on Computer and Communications Security*, 2019, pp. 973–990.

[22] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "Tales from the dark side : Privacy dark strategies and privacy dark patterns," in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2016, pp. 237–254.

[23] J. Luguri and L. Strahilevitz, "Shining a Light on Dark Patterns," *13 Journal of Legal Analysis 43*, 2021, university of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879, U of Chicago, Public Law Working Paper No. 719, Available at SSRN : https://ssrn.com/abstract=3431205 or http://dx.doi.org/10.2139/ssrn.3431205.

[24] 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 *ACM Conference on Human Factors in Computing Systems (ACM CHI)*, 2021, pp. 172 :1–172 :18.

[25] A. Mathur, M. Kshirsagar, and J. R. Mayer, "What makes a dark pattern... dark ? : Design attributes, normative considerations, and measurement methods," in *CHI*, 2021, pp. 360 :1–360 :18.

[26] Kevel (formerly Adzerk), "About us," n.d., https://www.kevel.co/about/ [Consulted on 29 April 2021].

[27] H. Brignull, “Dark patterns : User interfaces designed to trick people,” 2014, http://talks.ui-patterns.com/videos/dark-patterns-user-interfaces-designed-to-trick-people.

[28] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, “The dark (patterns) side of UX design,” in *Proceedings of the CHI Conference Human Factors in Computing Systems*, 2018, p. 534.

[29] M. Chromik, M. Eiband, S. T. Völkel, and D. Buschek, “Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems,” in *Intelligent User Interfaces Workshops*, ser. CEUR Workshop Proceedings, vol. 2327, 2019.

[30] D. Machuletz and R. Böhme, “Multiple purposes, multiple problems : A user study of consent dialogs after GDPR,” in *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, 2020, pp. 481–498.

[31] T. H. Soe, O. E. Nordberg, F. Guribye, and M. Slavkovik, “Circumvention by design – dark patterns in cookie consent for online news outlets,” in *NordiCHI*, 2020, pp. 19 :1–19 :12.

[32] Kevel (formerly Adzerk), “Consent Management Platform (CMP) 2021 Tracker,” n.d., https://www.kevel.co/cmp/ [Consulted on 11 February 2021].

[33] LiveRamp, “LiveRamp | Data Connectivity Platform,” https://liveramp.com/, [accessed on 20 May 2021].

[34] Liveramp, “Acxiom Marketing Solutions Sale Now Complete,” 2018, https://investors.liveramp.com/news-and-events/press-release-details/2018/Acxiom-Marketing-Solutions-Sale-Now-Complete/default.aspx.

[35] Cookie Script, “Cookie-Script : GDPR | CCPA | ePR cookie compliance solution,” https://cookie-script.com/, [accessed on 20 May 2021].

[36] Quantcast, “Quantcast Choice Supports TCF v2.0; Leading Consent Management Platform Now Offers Full Range of Premium Features in Free Solution,” n.d., https://www.quantcast.com/about-us/press/press-release/quantcast-choice-supports-tcf-v2/ [Accessed on 20 May 2021].

[37] Mozilla Corporation, “Dedicated profiles per Firefox installation,” https://support.mozilla.org/en-US/kb/profile-manager-create-remove-switch-firefox-profiles, [accessed on 20 May 2021].

[38] V. Wesselkamp, I. Fouad, C. Santos, Y. Boussad, N. Bielova, and A. Legout, “In-depth technical and legal analysis of tracking on health related websites with ERNIE extension,” in *Proceedings of the 20th Workshop on Privacy in the Electronic Society (WPES)*, 2021, pp. 151–166.

[39] I. Fouad, N. Bielova, A. Legout, and N. Sarafijanovic-Djukic, “Missed by filter lists : Detecting unknown third-party trackers with invisible pixels,” in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, no. 2, 2020, pp. 499–518.

[40] Commission Nationale Informatique et Libertés (CNIL), “Nouvelles règles pour les cookies et autres traceurs : bilan de l’accompagnement de la CNIL et actions à venir,” 2021, https://www.cnil.fr/fr/nouvelles-regles-cookies-et-autres-traceurs-bilan-accompagnement-cnil-actions-a-venir.

[41] ——, “Délibération No 2020-092 du 17 septembre 2020 portant adoption d’une recommandation proposant des modalités pratiques de mise en conformité en cas de recours

aux « cookies et autres traceurs »," 2020, https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf.

[42] H. Brignull, "Dark patterns," 2018, https://www.darkpatterns.org.

[43] A. Mathur, G. Acar, M. Friedman, E. Lucherini, J. R. Mayer, M. Chetty, and A. Narayanan, "Dark patterns at scale : Findings from a crawl of 11k shopping websites," *Proceedings of the ACM Human-Computer Interaction*, vol. 3, 2019.

[44] Commission Nationale Informatique et Libertés (CNIL), "On the practical procedures for collecting the consent provided for in article 82 of the french data protection act, concerning operations of storing or gaining access to information in the terminal equipment of a user (recommendation "cookies and other trackers")," https://www.cnil.fr/sites/default/files/atoms/files/draft_recommendation_cookies_and_other_trackers_en.pdf.

[45] IAB Europe, "TCF v2.0 CMP Service List," 2021, https://iabeurope.eu/cmp-list/.

[46] ——, "Vendor List TCF v2.0," 2020, https://iabeurope.eu/vendor-list-tcf-v2-0/.

[47] CookiePro by OneTrust, "Simple Pricing," n.d., https://www.cookiepro.com/pricing/ [Consulted on 27 April 2021].

[48] ——, "CookiePro," n.d., https://www.cookiepro.com/ [Consulted on 5 March 2021].

[49] Quantcast, ""Contact us" form," n.d., https://www.quantcast.com/#contact [Consulted on 6 April 2021].

[50] Liveramp, ""Talk to an Expert" form," n.d., https://liveramp.com/contact [Consulted on 6 April 2021].

[51] Commission Nationale Informatique et Libertés (CNIL), "Délibération No 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération No 2019-093 du 4 juillet 2019," 2020, https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf.

[52] noyb, "News Sites : Readers need to "buy back" their own data at an exorbitant price," 2021, https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price [Consulted on 26 Nov. 2021].

[53] Quantcast, "Quantcast Choice – User Guide," Apr 2021, https://help.quantcast.com/hc/en-us/articles/360052725133-Quantcast-Choice-User-Guide [Consulted on 30 May 2021].

[54] ——, "Quantcast Choice - Universal Tag Implementation Guide (TCF v2)," 2021, https://help.quantcast.com/hc/en-us/articles/360052746173-Quantcast-Choice-Universal-Tag-Implementation-Guide-TCF-v2-.

[55] Quantcast, "Privacy Policy," 2020, https://www.quantcast.com/privacy/.

[56] M. Veale and F. Z. Borgesius, "Ad tech and Real-Time Bidding under European Data Protection Law," *German Law Journal*, 2021.

[57] Commission Nationale Informatique et Libertés (CNIL), "Data & Design by LINC-CNIL : Co-building user journeys compliant with the GDPR and respectful of privacy," https://design.cnil.fr/en/.

[58] Y. Dimova, G. Acar, L. Olejnik, W. Joosen, and T. V. Goethem, "The CNAME of the game : Large-scale analysis of DNS-based tracking evasion," in *Proceedings on Privacy Enhancing Technologies*, vol. 2021, 2021, pp. 394–412, https://www.sciendo.com/article/10.2478/popets-2021-0053.

[59] Lauren Wakefield and Helen Mussard, "A Guide to the Post Third-Party Cookie Era," IAB Europe, Tech. Rep., Feb 2021, https://iabeurope.eu/knowledge-hub/iab-europe-guide-to-the-post-third-party-cookie-era-updated-in-february-2020/.

[60] Heinz Baumann, "Our view on a post-cookie world and identity," Feb 2021, https://www.quantcast.com/blog/our-view-on-a-post-cookie-world-and-identity/.

[61] The Trade Desk, "What the Tech is Unified ID 2.0 ?" Feb 2021, https://www.thetradedesk.com/us/news/what-the-tech-is-unified-id-2-0.

[62] Bruce Biegel and Charles Ping, "Collaborative Data Solutions : The Evolution of Identity in a Privacy-First, Post-Cookie World," Jan 2021, https://liveramp.com/lp/eb/collaborative-data-solutions-evolution-identity-privacy-first-post-cookie-world-eb-ty/.

[63] V. Mishra, P. Laperdrix, A. Vastel, W. Rudametkin, R. Rouvoy, and M. Lopatka, "Don't count me out : On the relevance of IP address in the tracking ecosystem," in *ACM International World Wide Web Conference (WWW'20)*, 2020, pp. 808–815.

[64] A. Gómez-Boix, P. Laperdrix, and B. Baudry, "Hiding in the Crowd : an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale," in *International World Wide Web Conference*, 2018, pp. 1–10, https://hal.inria.fr/hal-01718234.

[65] Criteo, "Identity Resolution & Criteo Shopper Graph Investor Presentation," 2019, https://criteo.investorroom.com/download/December+2019_Criteo+Shopper+Graph.pdf [Consulted on 30 Sept. 2021].

[66] CNIL, "Alternatives aux cookies tiers : quelles conséquences en matière de consentement ?" 2021, https://www.cnil.fr/fr/alternatives-aux-cookies-tiers-quelles-consequences-en-matiere-de-consentement.

CHAPTER 6

Conclusion and Perspectives

6.1 Conclusion

Online tracking of users for statistical and marketing purposes has existed almost since the origins of the web, and has evolved with it. As privacy legislation strengthens, privacy concern grows among users, third-party cookies are increasingly blocked by default in browsers, and advertisers adapt by creating new tools. This is how Consent Management Platforms (CMPs) appeared, boosted by the entry into force of new regulations such as the EU General Data Protection Regulation (GDPR). CMPs allow website publishers to acquire consent management as a service from a third party provider, claiming to help publishers to comply with complex privacy regulations.

In this thesis, we started by shedding light on the complexity of the consent management interfaces offered by CMPs and the issues arised by certain specific types of designs, usually grouped under the name of "dark patterns". To this end, we have mobilised a dedicated method, interaction criticism, in order to feed a transdisciplinary reflection specifically on three types of designs : the cookie wall, the consent wall, and the reduced service. By this means, we have broken down the different phases of consent management by CMPs, and highlighted the interest of a dialogue between the legal, computer science, and human-computer interaction disciplines for the design of more ethical consent pop-ups (Chapter 3).

From a legal viewpoint, we have also analysed the role of CMPs with regard to the GDPR. Indeed, CMPs generally define themselves as Processors, but they often carry out personal data processing for which they themselves define the means and purposes, placing them de facto in the role of Controllers. By comparing the data processing carried out by popular CMPs, we have highlighted four situations in which CMPs have the role of Controllers : 1) when they include additional processing activities in their tools beyond those specified by the IAB Europe, 2) when they scan publisher's websites for tracking technologies and sort them into purpose categories, 3) when they control third-party vendors included in their consent pop-ups, and 4) when they deploy manipulative design strategies in the user interface of consent pop-ups (Chapter 4).

Finally, we systematically analysed how CMPs could influence, coerce, or manipulate website publishers through dishonest interface and design choices. By following the journey of a publisher who wanted to implement different services provided by five of the most popular CMPs, we went through the registration, configuration, and installation process, the default options, and the resulting pop-ups. Our in-depth analysis shed light on positive and negative impacts of several common default consent pop-ups and tracker scanning tools, the potential influence of CMPs' interfaces on website publishers, and the risk of non-compliant consent pop-ups deployment (Chapter 5).

6.2 Ongoing work : privacy analysis of Google Tag Manager

Another evolution in the area of Web tracking technologies in the last decade is the introduction of Tag Management Systems (TMS) (see Section 2.1.2. In this section, we describe our ongoing work (started in 2022) focusing on Google's TMS, Google Tag Manager (GTM) *.

Since its introduction in 2012, GTM has gained an overwhelming dominant place in TMS market and it is currently deployed in 42% of the top 1M websites [93]. It enables website publishers to manage embedded scripts (e.g., for advertising or analytics), called "tags", in a uniform and supposedly simple manner. This centralisation of tags under the control of GTM is presented by Google as highly beneficial for publishers, since it needs less programming skills, and gives publishers a key control on what tags are executed and under which conditions. However, we show below that the situation is more complex.

The legacy (2012) client-side GTM version makes use of a unique component called "Web container", where tags are executed in the context of the user's browser. The new (2020) server-side GTM variant involves a remote server where tags are deployed and executed. As visible in Figure 6.1, personal data is collected in the web container by a dedicated collector tag (e.g., the Google Analytics 4, GA4, tag), transmitted over the Internet to the remote server container, processed by a GA4 adaptor component, and handled to the tags if appropriate. Then, tags execute and potentially transmit data (e.g., personal data) to remote third parties. Note that although the GA4 collector/adaptor components are used to connect the web and server containers, no data is sent to Google Analytics servers by default.

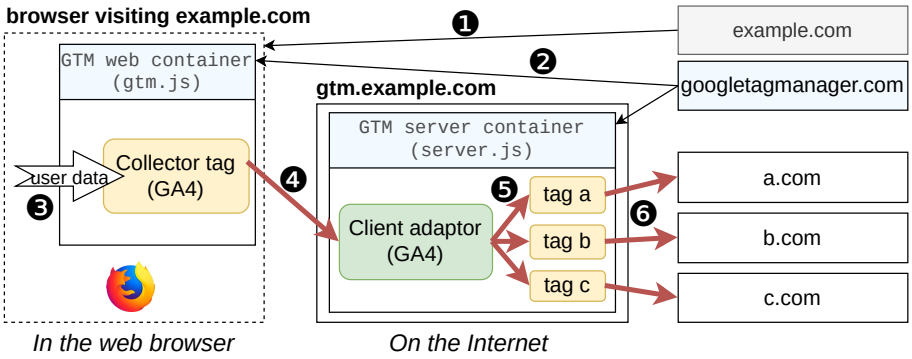


Figure 6.1 – **GTM server side architecture.** Data collected in the browser is sent to the remote server container where it is processed and potentially sent to third parties (data flows are shown with red arrows).

Privacy analysis of GTM Our ongoing privacy analysis of GTM follows several complementary directions. First of all, we analyze the journey of a publisher who includes and configures GTM in their website. Our goal is to identify identify the strategic advantages derived by Google and detail whether and how Google manipulates publishers by promoting their own tags and own cloud hosting facilities.

∗. This work is conducted with Gilles Mertens (since end 2022), Vincent Roca, Nataliia Bielova, Cristiana Santos (since March 2023) and Javiera Alegria-Bermudez (internship, March-June 2022).

On the one side, GTM does provide a key control to publishers over which tags are executed and how. For instance, its priority mechanism allows the publisher to define a strict order of execution between tags, to prioritize a consent pop-up tag and actively block other tags until the user makes their choice, which is beneficial to the end-user.

However, on the other side, GTM raises concerns. This is especially the case with server-side GTM that adds *obscurity-by-design* : moving tag execution to a remote infrastructure, out of reach of users, researchers and regulators, significantly limits the transparency of the targeted advertising ecosystem. This is in line with some blog posts published by digital marketing professionals and privacy activists [39, 41, 44]. For instance, publishers can leverage server-side GTM to hide the deployed tags and data transmissions to third parties. Publishers can also circumvent, or even prevent, the use of a browser privacy protection, by hiding the use of GTM, or by transforming cookies into first-party cookies. Doing so creates a major and structural loss of transparency, that directly benefits to a malicious publisher or third-party.

On the topic of consent, we also analyze the "Consent Mode" recently added by Google in the GTM. We investigate the consent management in the GTM and find out that its support is incomplete. First, on a client-side GTM, consent management is possible thanks to the recent *Consent Mode* option that the publisher can enable (e.g., for websites accessible to EU citizens). Google proposes "Consent variables" representing purposes for data collection by tags, and which can be obtained, for instance, through the interface of a consent banner. This system still raises questions, such as the formal semantics purposes, which is not clearly defined. For example, as of February 2023, Google documentation [94] describes the `ad_storage` purpose as : *"Enables storage (such as cookies) related to advertising"* and the `analytics_storage` as *"Enables storage (such as cookies) related to analytics e.g. visit duration"*. This description is not complete, given that several tags, such as user profiling ones, can present a large scale of actions that goes well beyond storage.

Second, there is no easy mechanism for all consent variables to be communicated to the server container (as of February 2023). The main approach relies on the GA4 exchange protocol, used to connect the browser and server containers. However, it is incoplete, and only manages the `analytics_storage` and `ad_storage` consent variables. Managing server-side tags requiring user consent for other purposes is therefore not possible on GTM.

Finally, similarly to our work on the role of CMPs (see Chapter 4), should Google be qualified a data controller or processor regarding GDPR ? A thorough legal study (with our legal colleague Cristiana Santos) is on progress to clarify Google status and responsibilities.

6.3 Perspectives

In this Section, we aim to give some insight about the most important work remaining to be done to improve the situation regarding consent management on the web. We summarize the major identified trends with associated privacy risks, and list our recommendations for the different stakeholders such as researchers, developers, and regulators.

Increased reliance on third-party providers Previous work on CMPs demonstrates their rapid expansion in the wake of new privacy regulations [70]. This switch towards an externalised management of consent requests by dedicated professionals could improve regulatory compliance and facilitate the dissemination of good practices. Previous research has shown that web developers

often include third-party content for tracking and non-tracking purposes [95], and that privacy is far from being their first consideration when making their choices [96]. Preliminary investigations made by journalists even indicates that, for instance, mobile application developers do not know what their applications is already doing [97]. Therefore, the risk exists that some publishers rely on third-party providers to manage trackers and user consent for them, without even knowing what data can be collected by their own services.

We believe it is important to continue research on third-party inclusions by evaluating trends and analysing the technical, legal, economic, and social impacts. The goal is to assess the consequences an increased reliance on third-party providers can have on privacy, and to determine the necessary adjustments to be made. This research should investigate how far publishers and developers are aware of the data processing of their websites and applications, especially since they are considered Data Controllers and legally responsible for the compliance with the law.

Global switch toward server-side tagging with Google Tag Manager The recent development of server-side tracking also raises questions. We have already explored server-side tracking in previous section, focusing on Google Tag Manager (GTM). This technology is presented as a gain in performance, security and privacy. However, it leads to significant changes in the execution of the JavaScript tracking code and the processing of personal data, as described in Section 6.2. Server-side execution makes it much easier to bypass the privacy protection features that are now built into most modern web browsers or available as extensions.

Following the highlights from the previous Section, we suggest in particular to shape future GTM studies around four questions :

- Does GTM facilitate user tracking, due to the simplicity of tag inclusion ?
- In a legacy website, do publishers replace vendor scripts with GTM tags altogether, or are both approaches used side by side, and with which consequences ? In particular, are user consent decisions obtained through a legacy CMP banner (in place before the addition of GTM) properly transferred to GTM tags (that rely on a totally different mechanism) ?
- How are the two versions of GTM used in practice ? Is server-side GTM used along with, or as a total replacement of client-side GTM ?
- Can we detect problematic situations, for instance that aim to hide a server-side GTM configuration ? Or when an essential feature is served through GTM to prevent a browser privacy protection to block GTM altogether ?

We believe it is required to set up large-scale measurements of Tag Management System (TMS) prevalence, and to develop new extensions to detect the use of TMS and tags, restrict data collection at the browser level, and be able to prove how user choices are stored and respected. A particular focus will be made to server-side GTM. This work can take a similar approach as the one of Matte et al. to detect consent violations with IAB TCF v1.1 [64].

Development of first-party data sharing Instead of direct connections from the user's browser to third parties, the personal data collection from server-side trackers could now happen directly on the servers, letting the browser and data visualisation tools in the dark. This loss of transparency is even more problematic as it seems to be followed by a global movement to encourage sharing of first-party data between companies by contractual agreements, also called "second-party data" [98]. Indeed, in 2023 all web browsers [28–30, 99] are already blocking third-party cookies except Google Chrome, and Google is planning to deprecate them in 2024 [31]. The announcement of the probable disappearance of third-party cookie, a powerful cross-site tracking

tool used by marketers, had a huge impact in the digital marketing and advertisement ecosystem, pushing companies to adapt to prevent the collapse of their revenue. Replacing traditional third-party tracking with first-party tracking, identity solutions, and second-party data is recommended by marketing professionals [100–103]. This semi-direct collaboration is based on the development of numerous new tools such as clean rooms, data cooperatives, data marketplaces [101], of logged environments, and "identity solutions" [103]. These data collections, carried out directly by the server during browsing, and then reconciled and shared by means of an identifier – generally a hash of an e-mail address [104, 105] – are taking place beyond the field of visibility of researchers, regulators, and end-users. Therefore, visitors and regulators can only rely on their trust in publishers and their data processors, and on their goodwill in terms of transparency and compliance.

From a technical viewpoint, researchers need to develop new methods for analysing such practices, from technical test-beds to large scale scans. From a regulatory viewpoint, policy makers and regulators also need to define clear guidelines at the European level. Strict regulatory controls will be necessary to prevent these large-scale data transfers to bypass consent requirements. At the user level, however, only the usage of temporary identifiers such as aliases, disposable mails, and virtual phone numbers [106] can prevent the cross-site matching of user data.

Ubiquitous data collection, from web to mobiles applications The development of the mobile web and related applications is also concerned. Google, for example, offers to include a GTM container as an SDK in Android and iOS applications [107]. The GTM SDK can then transmit data from the mobile device to the server container of a server-side GTM configuration. Companies such as LiveRamp propose at the same time consent management and online identity services [108, 109]. They enable matching of different sources of data using various identifiers, including mobile applications, making easier for advertisers to build profiles.

More research is needed to shed the light on these techniques, assess their implications on the end-users, and their legality. At the technical level, researchers need to do a technical assessment of the joint impact of mobile-based tracking, web-based tracking, and even physical in-store tracking, as well as assessment of available legal and technical protections are needed. At the economic level, they should seek to identify possible conflicts of interest and abuses of dominant positions by the major players in the web, mobile, and physical tracking industry. In some cases, those major players are indeed able to make their solutions de facto standards, which requires a critical assessment of the impacts. This is particularly the case for ubiquitous actors, as well as for companies acting simultaneously as consent management and identity providers, data brokers, and advertisers. It will certainly be necessary for regulators to adapt their guidelines and recommendations to take into account the recent changes in the ecosystem. In particular, we believe that regulators should assess the role of actors with multiple activities and potential conflicts of interest.

Long-term technical and social impacts These joint developments point to a future where the end of the third-party cookie tracking [31], far from signalling the end of so-called "surveillance capitalism" [110], would instead encourage its transition to new tracking tools that are more resistant to countermeasures, administered by data matching professionals. The shift in the balance of power between publisher and end-user leads to the fear of an obscure, closed data collection, depriving users, researchers, and regulators of means of understanding and auditing.

We believe that it is important to assess these impacts in a comprehensive way, and to adapt the technical and legal tools accordingly. On the technical side, both end-users, researchers, and

regulators would benefit from a simple interface (e.g., a browser extension) able to list tracking content embedded on a web site or application, even when hidden inside a tag manager, similarly to the work provided by Exodus Privacy on Android [111]. On the legal side, using a service such as a tag manager to prevent access to a website without tracking, or deliberately circumvent tracking protections and auditing, should be clearly banned. This work will benefit from a transdisciplinary dialog between technical and legal experts, and from a strong evaluation of the usability of the tools and methods with actual users. We, the research community, should work on the implications of these different services and practices as an analysis of a new global threat to privacy, and study the consequences of an evolution of the web towards moving the execution of trackers away from the user terminal.

Technical tools for at scale regulation Now more than ever, the upcoming large-scale development of new first-party and server-side tracking systems make it necessary for regulators to compare the technical behavior of sites and applications with declarations and specifications, such as privacy policies. Performing such analysis at scale will require semi-automated tools such as web crawlers. Besides detection of trackers themselves, we need to compare their behaviour to the legal declarations made by website publishers and third-parties in their privacy policies. These declarations are generally written in plain text, which make them hard to analyse at scale. In particular, extracting information from them with automated tools is not trivial [112]. Such processing would benefit from having a machine-readable description of privacy policies. It is therefore crucial to conduct an inventory of the needs in this area, to list the tools already available, and the development work that remains to be done. For researchers, it is also crucial to perform large scale analysis campaigns via these tools, to assess the situation and trends. This detection can also benefit from the use of common data description formats for collected data, commercial partners, associated purposes and legal basis. This modelisation can make use of semantic web ontologies, such as GConsent [113], or formal languages such as PILOT [114]. Finally, the representation of consent choices can be improved by building upon previous research on privacy policies [115]. For instance, a graphical depiction of purposes for data collection can help users to have a better understanding of their data sharing and its scope. This description could, for example, inspire from the DaPIS ontology-based icon set developed in 2018 by Rossi et al. [116].

Ethical design of privacy controls Work over the last decade has demonstrated the widespread presence of deceptive interfaces, now known as “dark patterns”. As we demonstrate in Chapter 5, in addition to end users, these unethical design choices can also influence website publishers. Recent regulatory changes in the EU contain legal limitations of dark patterns. The Digital Markets Act (DMA) [117, Article 5 and 6] contains an anti-circumvention rule regarding gatekeepers, while the Digital Service Act (DSA) [118, Article 23a] prohibit platforms to design any interface that *“deceives, manipulates or otherwise materially distorts or impairs the ability of recipients of their service to make free and informed decisions”*. However, it is now necessary to educate professionals to take privacy into account. Developers and designers need dedicated tools to evaluate interfaces and check their compliance with legal requirements. They can also be helped by a catalogue of examples of good and bad practices [119], created in an iterative and incremental approach, and informed by feedback from user studies. Regulators should probably also explicitly list examples of non-compliant design more actively than they do now, and formalise the conditions. Then, further experimentation of at scale non-compliant design detection can be made. However, the detection and categorisation of dark patterns is not an easy task, because of the complexity

of the notion itself as demonstrated by the numerous taxonomies [13, 14] produced over the last decade. Therefore, it is important to address the topic of ethical design from both a technical and regulatory viewpoint, involving several fields of expertise.

Importance of transdisciplinary work We have already worked together with researchers in design, computer science, and law through the interaction criticism method in Chapter 3, to build a constructive description of the complex and sometimes conflicting relations in the act of designing consent pop-ups. Beyond the privacy by design and by default, developing a "people-first by design" web, with ethics being taken into account from the design stage is probably the next necessary step. This cannot be done without a broad transdisciplinary collaboration involving HCI experts, lawyers, designers, economists, social and human sciences and computer scientists.

Bibliography

[1] Board of Trustees of the University of Illinois, NCSA, "NCSA Mosaic," https://www.ncsa.illinois.edu/research/project-highlights/ncsa-mosaic/ (Consulted on 4 Apr 2023).

[2] Google, "Benefits of online advertising and Google Ads," https://support.google.com/google-ads/answer/6123875?hl=en (Consulted on 4 Apr 2023).

[3] M. Zuckerberg, "Understanding Facebook's Business Model," 2019, https://about.fb.com/news/2019/01/understanding-facebooks-business-model/ (Consulted on 4 Apr 2023).

[4] B. Poilvé, "Les enchères en temps réel (RTB), un système complexe," 2020, https://linc.cnil.fr/fr/les-encheres-en-temps-reel-rtb-un-systeme-complexe (Consulted on 4 Apr 2023).

[5] "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009," 2009, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136.

[6] T. H. Soe, O. E. Nordberg, F. Guribye, and M. Slavkovik, "Circumvention by design-dark patterns in cookie consent for online news outlets," *NordiCHI '20 : Proceedings of the 11th Nordic Conference on Human-Computer Interaction : Shaping Experiences, Shaping Society*, 2020.

[7] H. Brignull, "Dark patterns : inside the interfaces designed to trick you," 2013, http://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you.

[8] ——, "Dark Patterns : User Interfaces Designed to Trick People," 2014, http://talks.ui-patterns.com/videos/dark-patterns-user-interfaces-designed-to-trick-people.

[9] H. Brignull, M. Miquel, J. Rosenberg, and J. Offer, "Dark patterns - user interfaces designed to trick people," 2015, http://darkpatterns.org/.

[10] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "Tales from the dark side : Privacy dark strategies and privacy dark patterns," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 4, pp. 237–254, 2016.

[11] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The Dark (Patterns) Side of UX Design," in *Proceedings of the CHI Conference Human Factors in Computing Systems*, 2018, p. 534.

[12] A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan, "Dark patterns at scale : Findings from a crawl of 11K shopping websites," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, p. Article No. 81, 2019.

[13] J. Luguri and L. Strahilevitz, "Shining a Light on Dark Patterns," *13 Journal of Legal Analysis 43*, 2021, university of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879, U of Chicago, Public Law Working Paper No. 719, Available at SSRN : https://ssrn.com/abstract=3431205 or http://dx.doi.org/10.2139/ssrn.3431205.

[14] C. M. Gray, C. Santos, and N. Bielova, "Towards a Preliminary Ontology of Dark Patterns Knowledge," in *Extended Abstracts of the 2023 ACM CHI Conference on Human Factors in Computing Systems (CHI EA '23)*, 2023.

[15] B. Krishnamurthy and C. E. Wills, "Privacy diffusion on the web : a longitudinal perspective," in *Proceedings of the 18th International Conference on World Wide Web*, 2009, pp. 541–550. [Online]. Available : https://doi.org/10.1145/1526709.1526782

[16] T. Libert, "Exposing the Invisible Web : An Analysis of Third-Party HTTP Requests on 1 Million Websites," *International Journal of Communication*, vol. 9, 2015.

[17] S. Englehardt and A. Narayanan, "Online tracking : A 1-million-site measurement and analysis," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, 2016, pp. 1388–1401.

[18] I. Fouad, N. Bielova, A. Legout, and N. Sarafijanovic-Djukic, "Missed by Filter Lists : Detecting Unknown Third-Party Trackers with Invisible Pixels," *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2020, 2020, published online : 08 May 2020, https://doi.org/10.2478/popets-2020-0038.

[19] "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) (Text with EEA relevance)," 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679.

[20] C. Santos, N. Bielova, and C. Matte, "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 (TechReg)*, pp. 91–135, 2020.

[21] "Evidence review of online choice architecture and consumer and competition harm," Competition and Markets Authority (CMA), Tech. Rep., 2022, accessed : 2022-4-13. [Online]. Available : https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers/evidence-review-of-online-choice-architecture-and-consumer-and-competition-harm

[22] Frobrukerrådet, "You can log out but you can never leave," 2021, https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf.

[23] Autorité de Protection des Données (APD), "Case DOS-2019-01377 – Decision on the merits 21/2022 of 2 February 2022 concerning complaint relating to Transparency & Consent Framework," 2022, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf.

[24] European Union Agency for Cybersecurity (ENISA), "Report on Data Protection Engineering," 2022, https://www.enisa.europa.eu/publications/data-protection-engineering/@@download/fullReport (Consulted on 17 Apr 2023).

[25] D. M. Kristol and L. Montulli, "RFC 2109 – HTTP State Management Mechanism," 1994, https://datatracker.ietf.org/doc/html/rfc2109.

[26] DataGrail, Inc., "The Great Privacy Awakening," 2022, https://www.datagrail.io/resources/interactive/2022-consumer-privacy-survey/.

[27] Commission Nationale Informatique et Libertés (CNIL), "Cookies equally easily accepted or refused : the CNIL sends a second series of orders to comply," 2021, https://www.cnil.fr/en/cookies-equally-easily-accepted-or-refused-cnil-sends-second-series-orders-comply (Consulted on 20 Mar 2023).

[28] Mozilla contributors, "Third-party cookies and Firefox tracking protection," https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-protection (Consulted on 20 Mar 2023).

[29] Brave Privacy Team, "Ephemeral third-party site storage," 2021, https://brave.com/privacy-updates/7-ephemeral-storage/ (Consulted on 20 Mar 2023).

[30] J. Wilander, "Full Third-Party Cookie Blocking and More," 2020, https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/ (Consulted on 20 Mar 2023).

[31] A. Chavez, "Expanding testing for the Privacy Sandbox for the Web," 2022, https://blog.google/products/chrome/update-testing-privacy-sandbox-web/ (Consulted on 20 Mar 2023).

[32] H. Shelley, "First-Party Data and Industry Collaboration Will Fuel the Post-Cookie Evolution of Digital," https://advertisingweek.com/first-party-data-and-industry-collaboration-will-fuel-the-post-cookie-evolution-of-digital/ (Consulted on 20 Mar 2023).

[33] P. Laperdrix, N. Bielova, B. Baudry, and G. Avoine, "Browser fingerprinting : A survey," *ACM Transactions on the Web (TWEB)*, vol. 14, no. 2, pp. 8 :1–8 :33, 2020, https://dl.acm.org/doi/10.1145/3386040.

[34] V. Mishra, P. Laperdrix, A. Vastel, W. Rudametkin, R. Rouvoy, and M. Lopatka, "Don't count me out : On the relevance of IP address in the tracking ecosystem," in *WWW '20 : The Web Conference 2020, Taipei, Taiwan, April 20-24, 2020*, 2020, pp. 808–815.

[35] Y. Dimova, G. Acar, L. Olejnik, W. Joosen, and T. van Goethem, "The CNAME of the Game : Large-scale Analysis of DNS-based Tracking Evasion," in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2021, pp. 394–412.

[36] Apple Inc., "Tracking Prevention in WebKit – Intelligent Tracking Prevention (ITP)," https://webkit.org/tracking-prevention/#intelligent-tracking-prevention-itp (Consulted on 20 Mar 2023).

[37] Brave Privacy Team, "Fighting CNAME trickery," 2020, https://brave.com/privacy-updates/6-cname-trickery/ (Consulted on 27 Feb 2023).

[38] R. Hill, "uBlock Origin works best on Firefox," 2020, https://github.com/gorhill/uBlock/wiki/uBlock-Origin-works-best-on-Firefox#cname-uncloaking (Consulted on 23 Feb 2023).

[39] J. Fedorovicius, "Introduction to Google Tag Manager Server-side Tagging," 2023, https://www.analyticsmania.com/post/introduction-to-google-tag-manager-server-side-tagging/ (consulted on 24 Feb 2023).

[40] S. Ahava, "Tags / Google Tag Manager," https://www.simoahava.com/tags/google-tag-manager/ (consulted on 22 Feb 2023).

[41] ——, "Agency, Transparency, And Control : Unsolved Problems With Server-side Tagging ," 2022, https://www.simoahava.com/analytics/agency-transparency-control-unsolved-problems-server-side-tagging/ (consulted on 24 Feb 2023).

[42] "Global Privacy Control (GPC) specification," 2023. [Online]. Available : https://privacycg.github.io/gpc-spec/

[43] Pixel de Tracking, "Notes sur l'extension du domaine de la surveillance (personal website)," https://www.pixeldetracking.com/ (consulted on 22 Feb 2023).

[44] ——, "Google Tag Manager, the new anti-adblock weapon," 2020, https://chromium.woolyss.com/f/HTML-Google-Tag-Manager-the-new-anti-adblock-weapon.html (English translated version).

[45] The European Parliament and the Council of the European Union, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," 2002, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (consulted on 29 Mar 2021).

[46] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

[47] N. Lomas, "How a small French privacy ruling could remake adtech for good," 2018, https://techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/ (Consulted on 17 Apr 2023).

[48] J. Ryan, "French regulator shows deep flaws in IAB's consent framework and RTB," https://brave.com/cnil-consent-rtb/, 2018.

[49] IAB Europe, "The CNIL's VECTAURY Decision and the IAB Europe Transparency & Consent Framework," 2018, https://iabeurope.eu/all-news/the-cnils-vectaury-decision-and-the-iab-europe-transparency-consent-framework/ (Consulted on 5 Apr 2023).

[50] Irish Council for Civil Liberties (ICCL), "Data Protection Authority investigation finds that the IAB Transparency and Consent Framework infringes the GDPR," 2020, https://www.iccl.ie/news/gdpr-watchdogs-investigation-finds-that-tracking-and-consent-pop-ups-used-by-google-and-other-major-websites-and-apps-are-unlawful/.

[51] Court of Justice of the European Union (CJEU), "Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH," 2019, http://curia.europa.eu/juris/documents.jsf?num=C-673/17.

[52] Commission Nationale Informatique et Libertés (CNIL), "Cookies : Google fined 150 million euros," 2022. [Online]. Available : https://www.cnil.fr/en/cookies-google-fined-150-million-euros

[53] ——, "Cookies : Facebook ireland limited fined 60 million euros," 2022. [Online]. Available : https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros

[54] Court of Justice of the European Union (CJEU), "C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems," 2020, https://curia.europa.eu/juris/document/document.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=4047220 (Consulted on 5 Apr 2023).

[55] Commission Nationale Informatique et Libertés (CNIL), "Utilisation de Google Analytics et transferts de données vers les États-Unis : la CNIL met en demeure un gestionnaire de site web," 2022, https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure.

[56] European Data Protection Board (EDPB), "Who are we ?" https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en (Consulted on 4 Apr 2023).

[57] ——, "Guidelines 05/2020 on consent, Version 1.1, adopted on 4 May 2020," 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[58] ——, "Report of the work undertaken by the Cookie Banner Taskforce, adopted on 18 January 2023," 2023, https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

[59] NOYB, "noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints," 2021, https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints (Consulted on 17 Apr 2023).

[60] Agencia Española de Protección de Datos (AEPD), "Guide on use of cookies," 2021, https://www.aepd.es/es/documento/guia-cookies-en.pdf (Consulted on 20 Mar 2023).

[61] Data Protection Commissioner (DPC), "Guidance note on the use of cookies and other tracking technologies," 2020, https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidancenoteoncookiesandothertrackingtechnologies.pdf.

[62] Information Commissioner's Office (ICO), "Update report into adtech and real time bidding," 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

[63] IAB Europe, "Vendor List TCF v2.0," https://iabeurope.eu/vendor-list-tcf-v2-0/ (Consulted on 4 Apr 2023).

[64] 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," in *IEEE Symposium on Security and Privacy*, 2020, pp. 791–809.

[65] 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 *CHI*, 2020.

[66] Kevel (formerly Adzerk), "About us," https://www.kevel.co/about/ (consulted on 29 Apr 2021).

[67] C. Matte, C. Santos, and N. Bielova, "Purposes in IAB Europe's TCF : which legal basis and how are they used by advertisers ?" in *Annual Privacy Forum, APF*, ser. Lecture Notes in Computer Science, 2020, https://hal.inria.fr/hal-02566891.

[68] S. Human and F. Cech, "A Human-Centric perspective on digital consenting : The case of GAFAM : Proceedings of KES-HCIS 2020 conference," in *Human Centred Intelligent Systems*, ser. Smart Innovation, Systems and Technologies, 2021, vol. 189, pp. 139–159.

[69] 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," in *Network and Distributed Systems Security Symposium*, 2019.

[70] M. Hils, D. W. Woods, and R. Böhme, "Measuring the Emergence of Consent Management on the Web," in *ACM Internet Measurement Conference (IMC'20)*, 2020.

[71] R. H. Thaler and C. R. Sunstein, *Nudge*. New Haven, CT and London : Yale University Press, 2008.

[72] R. H. Thaler, "Nudge, not sludge," *Science*, vol. 361, no. 6401, pp. 431–431, 2018. [Online]. Available : https://www.science.org/doi/abs/10.1126/science.aau9241

[73] A. Acquisti, "Nudging Privacy : The Behavioral Economics of Personal Information," *IEEE Security & Privacy*, vol. 7, no. 6, pp. 82–85, 2009.

[74] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The Dark (Patterns) Side of UX Design," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18, 2018, pp. 534 :1–534 :14.

[75] European Data Protection Board (EDPB), "Guidelines 3/2022 on dark patterns in social media platform interfaces : How to recognise and avoid them," European Data Protection Board (EDPB), Tech. Rep. Version 1.0, Mar. 2022. [Online]. Available : https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

[76] F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, and T. Rodríguez de las Heras Ballell, *Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report*. Publications Office of the European Union, May 2022. [Online]. Available : https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418

[77] "Bringing dark patterns to light staff report," Federal Trade Commission (FTC), Tech. Rep., Sep. 2022. [Online]. Available : https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

[78] "Dark commercial patterns," Organisation for Economic Co-Operation and Development (OECD), Tech. Rep., Oct. 2022. [Online]. Available : https://www.oecd-ilibrary.org/content/paper/44f5e846-en

[79] Frobrukerrådet, "Deceived by design : How tech companies use dark patterns to discourage us from exercising our rights to privacy," 2018, https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/.

[80] R. Chatellier, G. Delcroix, E. Hary, and C. Girard-Chanudet, "Shaping choices in the digital world," 2019, https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[81] E. Hary, "Dark patterns : quelle grille de lecture pour les réguler ?" 2019, https://linc.cnil.fr/dark-patterns-quelle-grille-de-lecture-pour-les-reguler.

[82] Information Commissioner's Office (ICO), "Guidance on the use of cookies and similar technologies," 2019, https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf.

[83] O. Kulyk, A. Hilt, N. Gerber, and M. Volkamer, ""This Website Uses Cookies" : Users' Perceptions and Reactions to the Cookie Disclaimer," in *European Workshop on Usable Security (EuroUSEC)*, 2018.

[84] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(un)informed consent : Studying GDPR consent notices in the field," in *Conference on Computer and Communications Security*, 2019, pp. 973–990.

[85] M. Chromik, M. Eiband, S. T. Völkel, and D. Buschek, "Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems," in *Intelligent User Interfaces Workshops*, ser. CEUR Workshop Proceedings, vol. 2327, 2019.

[86] 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*, ser. CHI '20, 2020, pp. 1–13.

[87] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems : A user study of consent dialogs after GDPR," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 481–498, 2020.

[88] 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 *ACM Conference on Human Factors in Computing Systems (ACM CHI)*, 2021, pp. 172 :1–172 :18.

[89] A. Mathur, M. Kshirsagar, and J. R. Mayer, "What makes a dark pattern... dark ? : Design attributes, normative considerations, and measurement methods," in *CHI*, 2021, pp. 360 :1–360 :18.

[90] Y. Acar, S. Fahl, and M. L. Mazurek, "You are Not Your Developer, Either : A Research Agenda for Usable Security and Privacy Research Beyond End Users," in *2016 IEEE Cybersecurity Development (SecDev)*, 2016, pp. 3–8.

[91] M. Tahaei, A. Frik, and K. Vaniea, "Deciding on Personalized Ads : Nudging Developers About User Privacy," in *SOUPS*, 2021.

[92] M. Toth, N. Bielova, and V. Roca, "On dark patterns and manipulation of website publishers by CMPs," in *Proceedings on Privacy Enhancing Technologies Symposium*, vol. 2022, no. 3, 2022, pp. 478–497.

[93] BuiltWith® Pty Ltd, "Tag Management Usage Distribution in the Top 1 Million Sites," 2023, https://trends.builtwith.com/widgets/tag-management (Consulted on 23 Feb 2023).

[94] Google, "Consent configuration," https://support.google.com/tagmanager/answer/10718549?hl=en (Consulted on 23 Feb 2023).

[95] D. F. Somé, N. Bielova, and T. Rezk, "Control What You Include ! Server-Side Protection Against Third Party Web Tracking," in *International Symposium on Engineering Secure Software and Systems*, 2017, pp. 115–132. [Online]. Available : https://hal.inria.fr/hal-01649547

[96] C. Utz, S. Amft, M. Degeling, T. Holz, S. Fahl, and F. Schaub, "Privacy Rarely Considered : Exploring Considerations in the Adoption of Third-Party Services by Websites," in *Proceedings on Privacy Enhancing Technologies*, vol. 2023, no. 1, 2023, pp. 5–28.

[97] K. Waddell, "Some Developers Don't Know What Their Apps Do With Your Data. Here's Why." https://www.consumerreports.org/privacy/developers-dont-know-what-their-apps-do-with-your-data-a1055672912/ (Consulted on 11 Apr 2023).

[98] C. Banashek, "Understanding the Language of Data," https://www.iab.com/blog/understanding-the-language-of-data/ (Consulted on 11 Apr 2023).

[99] Microsoft Edge Team, "Tracking prevention in Microsoft Edge," 2023, https://docs.microsoft.com/en-us/microsoft-edge/web-platform/tracking-prevention (Consulted on 20 Mar 2023).

[100] IAB Europe, "IAB Europe Guide to the Post Third-Party Cookie Era," 2021, https://iabeurope.eu/knowledge-hub/iab-europe-guide-to-the-post-third-party-cookie-era/ (Consulted on 11 Apr 2023).

[101] Winterberry Group, "Collaborative Data Solutions : Data and Identity in the Era of Permission," 2021, https://www.iab.com/wp-content/uploads/2021/05/Winterberry-Group-Collaborative-Data-Solutions-Final.pdf (Consulted on 11 Apr 2023).

[102] H. Baumann, "Our View on a Post-Cookie World and Identity," 2021, https://www.quantcast.com/blog/our-view-on-a-post-cookie-world-and-identity/ (Consulted on 11 Apr 2023).

[103] J. McDermott, "What the Tech is Unified ID 2.0 ?" 2021, https://www.thetradedesk.com/es/news/what-the-tech-is-unified-id-2-0 (Consulted on 11 Apr 2023).

[104] LiveRamp, "Hashing Identifiers," https://docs.liveramp.com/connect/en/hashing-identifiers.html (Consulted on 11 Apr 2023).

[105] ——, "Formatting Identifiers," https://docs.liveramp.com/connect/en/formatting-identifiers.html (Consulted on 11 Apr 2023).

[106] T. Klosowski, "How a Burner Identity Protects Your Inbox, Phone, and Credit Cards," 2021, https://www.nytimes.com/wirecutter/blog/how-to-disposable-email-phone-numbers-credit-cards/ (Consulted on 11 Apr 2023).

[107] Google, "Google Tag Manager for Android," https://developers.google.com/tag-platform/tag-manager/android/v5?hl=en (Consulted on 5 Apr 2023).

[108] LiveRamp, "Identity Resolution," https://docs.liveramp.com/identity/en/identity-resolution.html (Consulted on 11 Apr 2023).

[109] ——, "Interpreting RampID, LiveRamp's People-Based Identifier," https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html (Consulted on 11 Apr 2023).

[110] S. Zuboff, *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power*, 1st ed. Profile Books, 2018.

[111] "Exodus Privacy : Analyzes privacy concerns in Android applications," https://exodus-privacy.eu.org/en/ (Consulted on 11 Apr 2023).

[112] I. Fouad, C. Santos, F. A. Kassar, N. Bielova, and S. Calzavara, "On Compliance of Cookie Purposes with the Purpose Specification Principle," in *IEEE European Symposium on Security and Privacy Workshops (IWPE), EuroS&P Workshops 2020*, 2020, pp. 326–333.

[113] H. J. Pandit, C. Debruyne, D. O'Sullivan, and D. Lewis, "Gconsent - A consent ontology based on the GDPR," in *ESWC*, ser. Lecture Notes in Computer Science, vol. 11503, 2019, pp. 270–282.

[114] V. Morel, M. Cunche, and D. L. Métayer, "A generic information and consent framework for the iot," in *TrustCom/BigDataSE*. IEEE, 2019, pp. 366–373.

[115] V. Morel and R. Pardo, "SoK : Three Facets of Privacy Policies," in *Workshop on Privacy in the Electronic Society*, 2020. [Online]. Available : https://hal.inria.fr/hal-02267641

[116] A. Rossi and M. Palmirani, "DaPIS : An Ontology-Based Data Protection Icon Set," in *Knowledge of the Law in the Big Data Age, Conference 'Law via the Internet'*, ser. Frontiers in Artificial Intelligence and Applications, vol. 317, 2018, pp. 181–195.

[117] "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)," 2022, https://eur-lex.europa.eu/eli/reg/2022/1925/oj (Consulted on 11 Apr 2023).

[118] "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)," 2022, https://eur-lex.europa.eu/eli/reg/2022/2065/oj (Consulted on 11 Apr 2023).

[119] Commission Nationale Informatique et Libertés (CNIL), "Data & Design by LINC-CNIL : Co-building user journeys compliant with the GDPR and respectful of privacy," https://design.cnil.fr/en/ (Consulted on 11 Apr 2023).

List of Figures