Linköping University | Department of Computer and Information Science
Master's thesis, 30 ECTS | Information Technology
2022 | LIU-IDA/LITH-EX-A--22/072--SE

Bridging the Privacy Gap

– a proposal for enhanced technical mechanisms to strengthen users' privacy control online in the age of GDPR and CCPA

Överbryggande av integritetsgapet - ett förslag till förbättrade tekniska mekanismer för att stärka användarnas integritetskontroll online i en tid av GDPR och CCPA

Carl Magnus Bruhner

Examiner : Niklas Carlsson

LINKÖPING UNIVERSITY

Linköpings universitet
SE–581 83 Linköping
+46 13 28 10 00 , www.liu.se

Abstract

In the age of the *General Data Protection Regulation* (GDPR) and the *California Consumer Privacy Act* (CCPA), privacy and consent control have become even more apparent for every-day users of the internet. Privacy banners in all shapes and sizes asks for your permission through more or less challenging designs and makes privacy control more of a struggle than actually helping the users' privacy.

This thesis presents a novel solution expanding on the *Advanced Data Protection Control* (ADPC) mechanism in order to bridge current gaps in user data and privacy control. It moves the consent control to the browser interface to give a seamless and hassle-free experience for users, while at the same time offering content providers a way to be legally compliant with legislation including the GDPR.

Motivated by an extensive academic review to evaluate previous work and identify current gaps in user data control, the aim of this thesis is to present a blueprint for future implementation of suggested features to support privacy control online for users globally.

Acknowledgments

Despite the motivation of *"Don't do today what you can put off until tomorrow"*, as the great procrastinator Frankamin Benjlin famously said[1], the fear of not being invited to the official graduation ceremony with my classmates—who have played an integral role of these past years—ultimately caught up. As if by magic, my thesis was suddenly completed.

I would like to express my deepest appreciation and gratitude to my examiner and supervisor, Niklas Carlsson. Without his support, my foolhardy and/or ingenious endeavors of finishing all-but-thesis one year early, moving to Stockholm, and starting a full-time job while at the same time trying to finish up what got left behind, would not have been possible. His central role in my academic education cannot be overstated, and I am very thankful for all support, feedback, and cooperation throughout these years.

I am also grateful to friends and family for supporting my unorthodox attempts of combining my new cybersecurity career path while still spending several extended weekends on non-social thesis work. That is the struggle of a 33-year-old student, never really growing up.

Lastly, I'd like to acknowledge the great university life of Linköping and everyone that have been a part of it. Without you, my academic years would have been significantly more dull.

[1] Or *"Don't put off until tomorrow what you can do today."*, Benjamin Franklin? I'll look it up.. Tomorrow.

Contents

List of Figures

List of Tables

1 Introduction

Have you ever browsed the web, visiting one new website after another, only to find yourself heated up over getting bombarded with cookie and privacy banners? You are not alone. In 2021, United Kingdom's *Information Commissioner's Office* (ICO) called on the G7 countries to tackle the *"cookie pop-ups challenge"* by working to *"overhaul cookie consent pop-ups"* and *"provide a better web browsing experience"* [77]. Earlier that year, the non-profit privacy-enforcement organization NOYB, European Center for Digital Rights, announced an aim to end *"cookie banner terror"*, issuing over 500 GDPR complaints [26].

That being said, there has been a lot of previous work on privacy and consent, and new solutions are constantly evolving [43, 68]. With the introduction of modern privacy legislation, including the European GDPR and Californian CCPA, even more pressure has been put on data and service providers to ensure valid consent for collecting user information [92, 76].

Cookie banners are generally far from being legally compliant [36, 94], and incorrect consent signals can spread and threaten user privacy on a large scale due to connected consent management providers [61]. Even though GDPR and European legislators explicitly mentions browser settings as a way to express consent [85, 87], there has not yet been any widespread or compliant support [92] even though it can be considered the best solution for managing cookie consent [94].

This thesis presents a proposal for consent management in the browser, based on legal and technical requirements derived from research and based on existing protocols and mechanisms.

1.1 Motivation

Over the last five years, much have changed in terms of legislation—especially in the European Union with the GDPR, enforceable since 2018. This has led to reactions and adaptions from website and online advertisement providers in order to comply with the law. Nevertheless, almost nothing has changed from a browser and protocol perspective. Research has provided interesting new solutions [43, 68], especially within the field of machine learning [4, 13, 49], but still without the solutions making their way into every-day use.

The current state of privacy control is everything but satisfactory. Research shows that there are a large number of different solutions, with most—if not every—not complying with legislation. Some solutions are also very cumbersome for the end-user to customize, which rather results in a more limited or prevented user control.

A browser implementation could from a user perspective save time, make it easier, and enforce privacy rights. For a website provider and data controller, it could ensure legal compliance and ensure that the information and consent is correctly presented and expressed.

"No one shall be subjected to arbitrary interference with his privacy" as declared in the UN Declaration of Human Rights [107, Art. 12], and that together with the reality of privacy control and cookie consent banners constitutes the motivation behind this thesis.

1.2 Aim

The main idea of this thesis is to present a proposal for usable privacy features where the user is put in control. Previous standards, research and concepts that were ahead of their time are used as ideas and a foundation to present a novel solution where browser-based consent mechanisms are used to ensure compliance with privacy regulations such as GDPR and CCPA.

1.3 Research questions

As there have been numerous privacy and consent mechanisms presented since the dawn of the world wide web, a thorough literature review is required in order to utilize existing knowledge and techniques. Current challenges and solutions also needs to be identified to find what gaps are still prevalent and needs to be addressed. As means to bridge the gap of current privacy challenges and present a proposal for usable privacy features to put users in control, the following research questions have been formulated:

1. What are the current challenges and requirements of user privacy control online?
2. How can browser-based consent mechanisms provide conditions for legal compliance?
3. What features of a browser-based consent mechanism are required to bridge current gaps, and what are the steps needed to implement them?

Based on the answer to these questions, a proposal of features based on an existing browser-based consent mechanism is presented together with an implementation roadmap, feature dependency and division of responsibilities per stakeholder.

1.4 Contributions

The contribution this thesis makes is three-fold:

1. Presents a set of required properties of consent mechanisms, derived from legal requirements and research suggestions (Chapter 4)
2. Formulates requirements for browser-based consent mechanisms, based on the aforementioned properties (Chapter 5)
3. Suggests a set of features building on the *Advanced Data Protection Control* (ADPC), including an implementation roadmap to help pave the way for the future (Chapter 6)

Aside from the above contributions, a thorough research review is presented in Section 4.1, and a gap analysis of current and previous browser-based consent mechanisms in Section 5.2. Additional ideas of features and future work are presented in Section 9.1 and Appendix A.1.

1.5 Delimitations

The work of this thesis closely relates to the legal domain, but it does not claim to be a work within it. Instead, the study fully relies on research within the technical–legal domain as well as current legislation. As an effect of that, some legislative concerns have been omitted from the study, including explicit consent, imbalance of power in freely given consent, children's consent, and the exceptions of GDPR. These have also been omitted from the work of Santos et al. [92], which is of central importance in this thesis. Furthermore, the solution focuses on GDPR, thus leaving CCPA and other legislation outside the immediate scope, even though the legal requirements are still discussed in the thesis.

The thesis work has not aimed to provide any code or similar technical artifacts to be used for implementation of the solution. Instead, the aim is to provide concrete feature explanations that can be adapted, leaving the implementation of a working prototype as a suggestion of future work.

The suggested features are formulated as improvements to an existing browser-based mechanisms, ADPC. This is an intended choice, in contrast to other alternatives such as creating a new solution from scratch or utilizing multiple mechanisms. In selecting ADPC, a handful of the most prominent consent mechanisms, but not all, have been considered.

1.6 Thesis outline

In order to aid the understanding of the thesis, we begin with introducing some important concepts and background in Chapter 2. The chapter is divided in a non-technical part, beginning with Privacy in Section 2.1; and a technical part, beginning with the Hypertext Transfer Protocol in Section 2.4. The background is summarized in Section 2.10, before presenting the method of the thesis in Chapter 3.

Chapter 4 reviews the current state of web privacy based on research, presenting recommendations for improvements and legal requirements that are condensed into properties. Chapter 5 reviews the identified properties and compares browser-based consent mechanisms to determine a foundation, formulate requirements, and suggest improvements that need to be addressed for an ideal solution. Chapter 6 puts it all together, presenting suggested features, incentives and effects on affected parties, an implementation roadmap, and an evaluation of the result, which is further discussed in Chapter 7. Before we round off, we make an outlook on related and similar research in Chapter 8 and then finally concludes in Chapter 9 with a brief summary, and suggestions for future work.

Additionally, some supplementary suggestions can be found in Appendix A.

2 Background

Non-technical background

In this first part of the chapter, the aim is to introduce a few non-technical concepts around privacy and legislation that are of use for the remainder of the background and thesis.

2.1 Privacy

Unlike secrecy and authenticity, privacy is not a security requirement but a fundamental social right [17]. Not being subject of arbitrary interference of one's privacy is the twelfth article of the UN Declaration of Human Rights [107], which makes privacy not only a technical challenge—which is the scope of this thesis—but a political and legislative challenge as well. The technical and legislative development affect each other, with technical solutions adapting to legislation and, vice versa, gaining support from legislation as well [15, 43].

The complexity of privacy is also highlighted by the fact that anonymity is not enough to assure privacy, as public attributes, statistics, and correlations can be used to derive private attributes even without identifying persons [17].

Privacy policies on the web are one example of a battle between technical support and legislation, where privacy policies tend to be too complex with widespread misconceptions [103]. As if this was not enough, studies show that the privacy policies rather tend to increase in length and stay at high reading levels even after newer legislation [103].

2.2 Privacy legislation

With legislation identified as one of the main drivers for enhancing privacy, we will now scratch the surface of some of the more dominant legislation in this area that have been and are still being used around the globe.

2.2.1 The evolution of European privacy legislation

In 1995, the *Data Protection Directive* (DPD) [84] was passed, introducing directives on processing of personal data and free movement of such data—being the first EU-wide legislation of its kind [55]. The DPD farsightedly stated that *"the coordinated introduction of new*

telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data" [84, Rec. 6], and introduced definitions on natural persons, transparency, and consent [55].

Informed consent and giving users the option to opt-out of local data storage was introduced through the *EU Directive on privacy and electronic communications*, or *ePrivacy Directive* (ePD) [82], in 2002 [55]. The directive was a pioneer in specifically addressing cookies and the concerns around privacy and data protection, even though the directive had its issues in terms of interaction with the DPD and gaps in areas such as guidance and exceptions [24].

To address the gaps, the ePD was expanded in 2009 with the so-called "Cookie Amendment" [83], introducing explicit consent requiring user consent for cookies, unless strictly necessary for required services [91]. The consent was now required to be given *before* profiling technologies such as cookies was used, and through that lay the foundation for cookie banners [55, 105].

There have been several other EU-wide legislations in this area since, like the *Technical Regulations Information System* (TRIS) [80] preventing technical barriers between countries from arising, and the *European Electronic Communications Code* (EECC) [81] to harmonize the regulatory framework in the European Union.

2.2.2 Enter GDPR

The legislation that has really come to have a big impact on user privacy is the *General Data Protection Regulation* (GDPR) [85], passed in 2016 and effective as of May 2018. One major difference in comparison with previous legislation lies within the distinction between *directive* and *regulation*: directives need to be implemented in each member state's national law, whereas regulations are directly enforceable in all each EU member state [61]. Furthermore, the 34 articles of the predecessor DPD was increased to 99 articles in GDPR, aiming to be more precise than previous directives. However, there are critics that argue that some valuable former articles and guidelines have not been incorporated [89].

According to the European Commission, the intention with GDPR is to follow the approach of DPD with a modernization and legal harmonization within EU to strengthen individual's rights and control over personal data [20]. Another heavy key factor of the GDPR is that it introduces the power to impose fines of up to EUR 20 million—or 4% of worldwide annual turnover for companies—on controllers and processors [20].

To assist with support of applying the GDPR and other previous directives, as well as harmonizing between member states, there has been a working group called the *Article 29 Working Party* (WP29), named after the group being established in the 29th article of the DPD: *"Working Party on the Protection of Individuals with regard to the Processing of Personal Data"* [84, Art. 29]. WP29 was composed of representatives of data protection authorities from each member state and established EU authority as well as the European Commission. The group served as an advisory board, investigating questions regarding legislative application, advised the commission regarding amendments and supported with opinions on personal data protection. With the introduction and activation of GDPR, the WP29 has been succeeded by the *European Data Protection Board* (EDPB) [20].

In Sweden, national legislation has been introduced based on or related to EU directives and regulations, for instance the Swedish Electronic Communications Act [46], based on the EU ePrivacy directive, and the Act containing supplementary provisions to the EU General Data Protection Regulation [47], supplementing the GDPR.

2.2.3 Non-European privacy legislation

Similar to the GDPR, the *California Consumer Privacy Act* (CCPA) [16] has recently had a notable impact on privacy in California and the US. CCPA aims at giving users the right to know what personal information is collected and how it is used and shared, to opt-out of selling

collected information, to have the information deleted, and to receive non-discriminating equal service even when exercising CCPA rights [15, 79]. The CCPA has been expanded through the *California Privacy Rights Act* (CPRA) of 2020 [98], also known as Proposition 24 relating to how it was presented and approved in 2020.

There have been several privacy laws in the US before, however jointly considered a *"complex patchwork of narrowly tailored federal and state laws"* [79]. For the protection of children, there have been both federal and state laws, with the *Children's Online Privacy Protection Act* (COPPA) of 1998, and the *California Online Privacy Protection Act* (CalOPPA) of 2003 being the most notable.

Widening the scope outside of the US, there are other privacy legislation around the world that can be of need to consider from a technical perspective: *Lei Geral de Proteção de Dados Pessoais* (LGPD) of Brazil, the *Personal Data Protection Act* (PDPA) of Singapore, and the *Consumer Privacy Protection Act* (CPPA) of Canada, to name some.

2.3 Consent

Consent is of central importance from a legislative perspective to determine what is and what is not allowed [44]. According to the definitions in GDPR, consent means *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"* [85, Art. 4(11)]. The DPD also used 'freely given', 'specific', 'informed' and 'unambiguous' to express valid consent [84].

Websites, including the major social media websites, have been found to not use a so-called human-centric perspective of enabling informed consent, but rather to utilize patterns steering the users into consenting [44]. From a technical perspective, consenting is possibly as complex as privacy. A recent study identified 22 legal–technical requirements for a valid consent, with several examples of violations each, regarding the use of cookies [92], a study we will return more to in coming chapters.

***

Technical background

In this second part of the chapter, the aim is to introduce various standards, protocols and other technical mechanisms that are or could be of use for strengthening the user privacy control.

2.4 Hypertext Transfer Protocol

Used since 1990, the *Hypertext Transfer Protocol* (HTTP) was first standardized as version 1.0 in 1996 [71]. HTTP is an application-layer protocol that defines a way of communicating messages between a client and a server over the transport layer. When visiting a website in a browser, HTTP is the mechanism that both requests and receives the web page data that is presented in the browser interface. The protocol has been evolving ever since its first version with version 1.1 published in 1997 [31] (updated 1999 [72] and 2014 [32]), version 2 in 2015 [10] and version 3 just around the corner[1], utilizing QUIC as transport layer protocol [12].

The importance of HTTP for the internet as we see it today can hardly be overstated, and it has been stated to be the foundation where new functionalities of the internet can and will be implemented [88]. The fact that newer versions of HTTP build upon the same semantics and functions, that nowadays have a separate specification [33], helps ensure this. The goal of newer versions of HTTP is instead to improve how the semantics can be communicated, i.e., mapped to different transport layer protocols.

[1] Actually, upon finalizing this thesis, HTTP/3 has officially been released as RFC 9114 in June 2022.

2.4.1 Well-Known Uniform Resource Identifiers (Well-Known URIs)

Well-Known *Uniform Resource Identifiers* (URIs) [73] are special URIs reserved for data related to a resource origin. The URI follows the host URI with `/.well-known/` followed by the specific well-known resource. For instance, if we wanted to make a fictitious well-known resource `ground-rules` available on our website `example.com`, we would host them at the URI `https://example.com/.well-known/ground-rules`. This would in this case allow for all browsers visiting our website to effortlessly locate the "ground rules" for our website. The registry of (real) well-known URIs are maintained by IANA and available online[2].

An actual well-known URI—however, confusingly not a well-known URI in this sense—is the `robots.txt` resource available at the root of each domain that wants to instruct how robots (i.e., crawlers) can and should access the website. Nevertheless, this resource is neither located in the designated path (`/.well-known/`) nor registered in the IANA registry. A similar initiative is `ads.txt` by IAB Tech Lab, used for programmatic advertising transparency [57].

2.4.2 HTTP header fields

HTTP packets contain a header with several fields, some required and some optional, that the host and sever use to communicate settings and preferences. For instance, a `GET` request from a browser that prefers a website to be displayed in Swedish might include the header `Accept-Language: sv-SE,sv`[3].

IANA have registries for permanent and provisional HTTP header field names[4], according to the informational memo on HTTP Header Field Registrations [74]. The permanent registry contains IETF-standardized header fields and other header fields of similar review or recognition (`Accept-Encoding` being one such example), whereas the provisional registry is open for any header field proposed by any developer and does not imply any endorsement [53].

2.4.3 Extensibility of HTTP

There are some other ways to extend HTTP available from within the HTTP standard, and we will now review a few of these possibilities.

Custom request methods

HTTP exchanges are initiated by one party (client) sending a request to the other party (server). The request is one of several predefined request types which indicates the purpose and what is expected in return. The `GET` request method, known from web browsing, is used to request a current representation of a given resource [33]—for instance retrieving a web page from a server. General-purpose servers need to support at least `GET` and `HEAD` requests, but there are an additional six optional request types standardized in the HTTP semantics [33]. Similar to header field names, IANA maintains a registry of HTTP methods[5]. Additional request methods can be created and used, even though they ought to be registered with IANA [33].

Custom response codes

When a client sends an HTTP request (`GET` for instance) to the server, the server sends a response containing a status code. The code is three digits and classified in five categories: `1xx` Informational, `2xx` Successful, `3xx` Redirection, `4xx` Client Error, and `5xx` Server Error [33]. In a traditional internet browsing example, a `200 OK` informs that the requested page

[2] `https://www.iana.org/assignments/well-known-uris/`

[3] The author's browser actually uses `Accept-Language: sv-SE,sv;q=0.9`, the last part being an optional relative *quality value* explained in the HTTP semantics [33] for readers eager to dig deeper into the subject.

[4] `https://www.iana.org/assignments/message-headers/`

[5] `https://www.iana.org/assignments/http-methods/`

was found and follows after the header, whereas a `404 Not Found` indicates that the requested resource could not be found at that location.

Standardized response status codes are defined in the HTTP semantics, and IANA maintains a status code registry[6] in this case as well. Additionally, response codes are extensible with the only requirement being that they follow the overall 1–5 classification. Following this, if a client receives an unknown `525` code, it can at least derive that there was an error at the server side even though the type of error might be unknown.

Server communication requests

One of the optional request methods that are defined in the HTTP semantics is the `OPTIONS` method [33]. This method allows for requesting information regarding communication options available at the responding side. It can either be requested for a specific resource by specifying it in the request, or server-wide by using an asterisk (*) as request target. The `OPTIONS` request method can be used in combination with other customizations in order to see if a server supports these customizations before trying to use them.

2.5 Cookies

HTTP is by design a stateless protocol, meaning that request messages should be possible to understand in isolation and independent of other factors such as connection [32]. In order to support states, a state management mechanism utilizing cookies was standardized in 1997 [66]. An updated standard using `Cookie2`, with support for specifying port numbers and comment URLs, was introduced in 2000 [67] but obsoleted by the current standard from 2011 [7].

The original specification had support for an optional `Comment` field to document its intended usage:

> *Because cookies can contain private information about a user, the* [Comment] *attribute allows an origin server to document its intended use of a cookie. The user can inspect the information to decide whether to initiate or continue a session with this cookie.* RFC 2109 [66, p. 4, with author's correction]

This was information that the user could review to decide whether to allow/continue or not. This was further expanded in Cookies2 with the `CommentURL` field that allowed for having the information at a separate URL [67]. The same standardization also emphasized the value of `Comment` and `CommentURL` by stating that servers *should* promote informed consent by including these fields; preferably the latter to provide more detailed information and in more languages. Furthermore, it stated that *"A user should be able to find out how a web site plans to use information in a cookie and should be able to choose whether or not those policies are acceptable"* [67, p. 18]. All of this was removed in the latest specification, instead adding a *Privacy Consideration* section with a few general-purpose *should*-rules (weaker than the binding *must*) such as that browsers *should* offer some kind of cookie manager as well as a possibility to disable cookies all together.

In the proposed fourth version of the HTTP State Management Mechanism, an additional `SameSite` attribute is introduced that makes it possible to set how a cookie can be accessed depending on if it is same-site or cross-site [18]. The strictest attribute, `SameSite=Strict`, for instance allows for requiring the visible URI in the user's browser to correspond to the requested cookie to prevent misuse. The proposed standard also suggests that IANA, analogously to previous standards, creates and maintains a Cookie Attribute Registry[7] where new entries can only be added through an RFC, in contrast to the earlier mentioned registries. Google Chrome

[6] `https://www.iana.org/assignments/http-status-codes/`

[7] `https://www.iana.org/assignments/cookie-attribute-names` (Does not exists at the time of this writing, but let's see who comes first to the finish line: the new cookie RFC or this thesis.)

began enforcing stricter policies regarding `SameSite` features in 2020, and slow adoption rate led to breakage of features due to Lax-by-default—primarily affecting advertising features [50].

2.5.1 Third-party, session and persistent cookies

There are some common characteristics used to describe different types of cookies, and that is first-party, third-party, session (non-persistent), and persistent cookies. The first group, first-/third-party, is defined by whether the cookie originates from the server directly visited (i.e., the URL visited by the user), or from another server from which the main server requests the user agent to fetch resources from [7]. If several websites include resources from the same third-party server—an ad server for instance—that server could use cookies to track the user between these sites.

The second group, session/persistent, is defined by the cookie's persistent-flag and whether it is set to true or false. The persistent-flag is a field that the user agent stores about the cookie that determines if the cookie should be removed when the session is over. It is automatically set to true if it contains a `Max-Age` or an `Expires` attribute, but defaults to false if those attributes are not present [7].

Both persistent and third-party usage is raised as privacy concerns in the cookie standard, of which third-party cookies are mentioned as "particularly worrisome" [7, p. 27].

2.5.2 Various types of cookies and their usage

Based on the characteristics above and the intended usage, there are some common categories and features of cookies:

- Strictly necessary cookies. According to the ePD, the requirement of user consent to store information locally in the user's equipment does not include such storage and access needed to enable communication or as "strictly necessary" to provide the services the user explicitly requested [82, Art. 5(3)]. This statement was repeated in the ePD cookie amendment, using the terms "legitimate interest" and "legitimate purpose" for the strictly necessary cases [83, Rec. 66].

- Preference/functionality cookies. Cookies that store user interface customization not linked to the user's profile and explicitly requested by the user through interaction [92]. Can be exempted from prior consent if session cookies are used, but not if persistent cookies are used.

- Analytics cookies. Used for statistical purposes and can be divided into two classes: local and non-local [92]. Local analytics, using first-party cookies, can to some extent be used without consent if anonymized. Non-local analytics, using third-party cookies, always require consent.

- Marketing cookies. Cookies with the purpose of advertising and using data for marketing in various ways. These cookies are not strictly necessary as they are usually not related to the service explicitly requested [92].

- Secure cookies. Defined by setting the `Secure` attribute and limits the scope of the cookie to secure channels like HTTPS [7]. The proposed cookie standard also introduces a `__Secure-` name prefix that always needs the `Secure` attribute to be set, and a `__Host-` name prefix that additionally forces the scope to be host-only (i.e., no `Domain` attribute) and the entire host instead of specific paths (i.e., the `Path` attribute set to '/') [18].

2.6 Browser-based consent mechanisms

There has been a number of initiatives throughout the years regarding policies, standards, etc. for user privacy and consent.

2.6.1 Platform for Privacy Preferences Project (P3P)

The *Platform for Privacy Preferences Project* (P3P) [22], originally drafted in 1999 and published in 2002, was a promising initiative for user privacy supported by both Microsoft Internet Explorer and Netscape Navigator [23]. Microsoft supported it all the way to Microsoft Edge, however removing support in 2016 [65] before W3C obsoleted P3P in 2018.

P3P standardized a way for websites to offer privacy policies so that, for instance, a browser can check whether the data collection the website requests (through P3P) is acceptable according to the user's setting and thus can be allowed with no interaction, or if the request goes beyond what is allowed by default and thus requires user interaction to be allowed.

Based on P3P, *A P3P Preferences Exchange Language* (APPEL) [21] was designed to allow for exchanging sets of preferences, called rulesets. The vision being to allow for downloading pre-defined rulesets from trusted parties and being able to share preferences between multiple user agents.

Additionally, there have been several other initiatives based on P3P, for instance an XPath-based alternative to APPEL [2] refined into the preference language XPref [3].

2.6.2 Do Not Track (DNT)

Do Not Track (DNT) [34], or Tracking Preference Expression, was also a W3C initiative for enabling user preferences. In short, it introduced the HTTP header field `DNT` where the browser could include the user's preference regarding tracking in the requests sent to the server.

The beginning of the end of DNT happened already back in 2012 when Microsoft shipped Internet Explorer 10 with DNT activated by default [35]. This was a violation of the intended design, where the user actively had to opt-out, giving website owners and advertisers the incentive to ignore the DNT header instead of respecting it (the Apache HTTP Server Project even briefly added a controversial work-around to ignore DNT for all Internet Explorer 10 users, committed by the DNT co-editor [30]). The Tracking Protection Working Group of W3C finally concluded its work in 2019, thus putting an official end to DNT [27].

The *Electronic Frontier Foundation* (EFF) expanded on the DNT initiative by creating a compliance policy utilizing the well-known URI structure for standardization [37]. This way a domain can communicate that it respects DNT.

2.6.3 Global Privacy Control (GPC)

Global Privacy Control (GPC) [11] is a privacy initiative anchoring on the CCPA and GDPR legislation with inspiration from the W3C DNT initiative. Especially inspired by CCPA, GPC aims at giving the user a way of expressing a "do not sell or share" preference using a `Sec-GPC` header field. Transmitting this preference to the server is supposed to signal an opt-out request according to CCPA regulations §999.315 [16]. The State of California Department of Justice Attorney General currently lists GPC as a way of submitting an opt-out request, thus validating GPC as a legal way of enforcing the CCPA regulations [15]. The timing of GPC in the new legislative landscape is a key difference to its predecessor DNT [43]. At the time of this writing, GPC is supported by the browsers Brave, DuckDuckGo, and Firefox[8].

[8] `https://globalprivacycontrol.org/`

2.6.4 Advanced Data Protection Control (ADPC)

Advanced Data Protection Control (ADPC) [45] is another privacy initiative aiming to be an alternative to cookie banners and similar manual consent management systems. In contrast to DNT and GPC, ADPC is not limited to a binary signal but instead customizable to allow for tailored needs. It also does allow both an opt-in and opt-out approach, in contrast to the opt-out approach of DNT and GPC. It uses GDPR as a basis for motivation but is open to use for other legislation as well. ADPC currently support HTTP and JavaScript for exchanging ADPC communication, with an `ADPC` header in HTTP to send ADPC signals to the server. At the time of this writing, ADPC has two prototype demo plug-ins available for Firefox and Chromium-based browsers[9].

2.7 Provider-based consent mechanisms

Aside from the browser-based consent technology, there has been some initiatives from the content providers as well, especially in the wake of the ePD cookie amendment and cookie policies. One category is consent management platforms that offer content providers functionalities like cookie banners and legal data processing conformity [55]. This transfers the consent management to a third party, a *Consent Management Provider* (CMP), even though the content provider should be considered to have equal responsibility in compliance [61].

One leading platform, considered to be a de facto standard [93], is the *Transparency & Consent Framework* (TCF) [28], standardized by the European branch of the *Interactive Advertising Bureau* (IAB) and since August 2019 available in its second iteration, v2.0. It aims to provide GDPR compliance for the digital advertising industry, even though the compliance has been widely questioned [39, 43, 61, 92, 93]. IAB Europe maintains a *Global Vendor List* (GVL) with registered advertisers that declares pre-defined purposes for data collection [61].

Technically, IAB uses the domain `consensu.org` where each provider has their own subdomain to be able to read and modify a shared cookie that handles consent information in compliance with the same-origin policy. However, this shared consent means that a violation of compliance can easily spread and thus invalidate the proof of consent offered by TCF [61].

Another initiative is the *Network Advertising Initiative* (NAI), which has been around for 20 years without being widely adopted (75 vendors as of 2021) [43]. It is similar to DNT and GPC but implemented as a website[10] that sets an opt-out cookie for all participating vendors.

2.8 User experience of privacy features

Another take on user privacy control is the resulting user experience, and the burden of being interrupted with consent dialogs for every initial visit to a website [41]. Using private browsing only makes the problem worse, increasing the interruptions to every initial visit of every new session. For user with visual disabilities, usability around online security and privacy has been found to be severely troublesome, putting users at significant risk [70].

A widespread phenomenon is the use of so called ”dark patterns”, designs that manipulatively steer user in a deceiving or predetermined direction such as accepting or selecting certain options in the case of cookie banners [39, 75]. Big tech companies like Google and Facebook have been found to utilize such dark patterns, instead of using cognitive dimension to empower end-users [44]. Examples of dark patterns include unequal paths, where the most and least privacy-protective choices have unequal interaction paths, and ”confirmshaming”, where wording uses guilt or shame to influence a decision [41]. As a reaction, both European and American legal initiatives have been taken to prohibit various dark patterns, including unequal paths where GDPR is requiring withdrawal of consent to be as easy as giving [75, 92].

[9] `https://www.dataprotectioncontrol.org/prototype/`
[10] `https://optout.networkadvertising.org/`

2.9 Other tracking and tracking prevention

Aside from what has already been mentioned, there are several other types of tracking and tracking prevention. A notable example is browser fingerprinting, a technique used by content providers to uniquely identify browser instances without the need to use cookies or similar [78]. Because of its nature, bypassing user consent and ability to decline, it violates GDPR and is more challenging to prevent or mitigate, even though it is possible.

To limit and prevent tracking, there are various techniques implemented by browser vendors in their browsers. Apple has *Intelligent Tracking Prevention* (ITP) [5] available through WebKit, the web browser engine used by Safari, and Mozilla has *Enhanced Tracking Protection* (ETP) [69] included as a feature of Firefox.

Other web initiatives include ad, script, tracking and content blockers, which works by altering the loaded website or in other ways blocking certain content from loading. As it infers with the website it is also detectable and can trigger websites to nudge for inactivation or to block the requested content from being served [64]. Ad blockers can however be deceiving, and a 2021 study showed that when ads were not present, users falsely assumed that there were no potentially intrusive practices going on due to this [97].

An example of a related but non-web initiative is Apple's *App Tracking Transparency* (ATT) policy, that requires developers to explicitly ask for permission when using information from other companies' apps to prevent undisclosed tracking [64].

***

Background summary

2.10 Summary

Privacy is a human right, and a technical complex matter. To ensure privacy, numerous legislations have been and are still evolving, including the recent extensive legislation GDPR and CCPA. A central concept regarding user privacy legislation is to safeguard user consent—a technical challenge this thesis aims to improve.

HTTP is one of the central protocols of the internet and stated to be the foundation for new functionalities. HTTP offers many possibilities for extension and standardization, including well-known URIs, custom header fields, request methods and response codes, and more. As HTTP is a stateless protocol by design, cookies are used to bridge the need for session data and similar. There are several characteristics and usages of cookies, including first and third party, session and persistent, necessary, secure, etc.

To strengthen users online, various initiatives and standardization has been proposed and implemented throughout the years. P3P, DNT, GPC, and ADPC are some examples, primarily browser-based on the user side, whereas TCF with cookie banners and NAI with opt-out cookies are examples of initiatives from the content and ad provider side. All-in-all, various initiatives and especially the cookie banner have created a challenging user experience that legislation now aims at mitigating. Additionally, more unsupported technical solutions on both sides such as browser fingerprinting and ad blockers are added to the equation, as well as browser vendors and platform providers with privacy preserving initiatives such as ITP and ETP.

Arguably, there are a lot of room for improvement in the area of user privacy control and consent online, and that is the topic for the remainder of this thesis.

2.11 Definitions

data controller
The entity that determines how and why personal data is processed. Examples: website owners, content providers *(see 'controller' in GDPR [85, Art. 4(7)])*

data subject
An identified or identifiable natural person [85, Art. 4(1)], e.g., users and website visitors.

legitimate interest
Legal basis for processing of personal data in some cases such as providing an explicitly requested service, preventing fraud, etc. *(see GDPR [85, Rec. 47])*

personal data
Any information relating to data subjects *(see 'personal data' in GDPR [85, Art. 4(1)])*

consent mechanisms
Technical way of offering privacy and consent control. Examples: browser signals, browser consent settings, cookie banners

2.12 Abbreviations

ADPC Advanced Data Protection Control (see Section 2.6.4)

CCPA California Consumer Privacy Act (see Section 2.2.3)

CMP Consent Management Provider (see Section 2.7)

DNT Do Not Track (see Section 2.6.2)

ePD EU Directive on privacy and electronic communications (see Section 2.2.1)

GDPR General Data Protection Regulation (see Section 2.2.2)

GPC Global Privacy Control (see Section 2.6.3)

HTTP Hypertext Transfer Protocol (see Section 2.4)

P3P Platform for Privacy Preferences Project (see Section 2.6.1)

TCF Transparency & Consent Framework (see Section 2.7)

URI Uniform Resource Identifiers (see Section 2.4.1)

WP29 Article 29 Working Party (see Section 2.2.2)

3 Method

The aim of this chapter is to briefly present how the thesis work has been conducted for the sake of replicability. Given the qualitative nature of this study, this might help explain how the study can be repeated and achieve a somewhat similar result.

3.1 Identifying relevant research

To begin with, an extensive literature search and review was conducted in order to present an as robust foundation as possible. For this, proceedings of several top-ranking and niche conferences; including *Symposium on Usable Privacy and Security* (SOUPS), *Privacy Enhancing Technologies Symposium* (PETS), *Workshop on Privacy in the Electronic Society* (WPES), *IEEE Symposium on Security and Privacy* (S&P) and its European counterpart (EuroS&P); has been manually reviewed to find relevant and recent papers. The ACM Digital Library and IEEE Xplore have, together with Google Scholar, been the main search engines used, with citations and similar quality factors utilized to find recognized research. For relevant papers, both tracing of citations and bibliography reviewing have been used to identify even more relevant papers. Keywords based on techniques, protocols and concepts have also been fine-tuned and experimented with to identify all relevant research within the area of web privacy, consent mechanisms, cookies, and legal compliance.

Aside from this, a general information seeking outside of the academic scope was of central value here in order to identify even more concepts and keywords that might not (yet) have found its way to more mainstream research.

3.2 Combining the findings and identifying the gaps

Based on the findings in relevant research, common patterns have been identified including recurring recommendations. The extensive legal–technical work by Santos et al. [92, 94], was chosen as central framework due to its multidisciplinary perspective and systematic division of legal requirements. In order to support this choice, other research was reviewed and mapped to provide additional support for the selected framework. That framework and recurring recommendations were then combined into a set of properties used as a benchmark of legal compliance going forward. This is presented in Chapter 4.

3.3 Benchmark and analysis to bridge the gaps

With the derived properties, potential identified browser-based consent mechanisms were benchmarked against them to compare and determine a suitable foundation for further improvements. The benchmark was made by assessing the property fulfillment of each property per mechanism with four potential values: fulfills, partly fulfills or usage-dependent, does not fulfill, or not applicable. The assessment was done through manual evaluation of documentation to assess how each mechanism fulfilled the properties. Based on this assessment, a solution was chosen based on fulfillment and current usage status.

Having selected a mechanism, the next step was to review all properties and suggest improvements that could be made based on current fulfillment for each of the properties. These suggestions were based on the identified gaps and the description of each property. This is presented in Chapter 5.

3.4 Recommendation and guidelines to put it all together

Using the set of properties with suggested improvements, multiple ideas were combined to suggest features that can be implemented by browsers, server software and data controllers. Each feature was created based on the originating research, legal requirement, and property descriptions.

Based on the suggested features, an implementation roadmap and a feature dependency map were designed to present how the features could be implemented. Finally, the result was evaluated by assessing the resulting property fulfillment with the new features. This is presented in Chapter 6.

4 Identifying the gaps in user privacy control

The aim of this chapter is to identify and present properties that need to be fulfilled for a legally compliant privacy control. We start with the current state of web privacy, identify legal requirements and recurring recommendations, and then combine them into a set of desirable properties that we will make use of going forward.

4.1 Current state of web privacy

Cookie usage and opting in/out: In 2019, Sanchez-Rola et al. [91] showed that more than 90% of visited websites used cookies that could identify users. Furthermore, the study found opting out from tracking to be both difficult and ineffective due to opt-out features not being properly implemented, leaving users tracked with long-lasting cookies.

Smullen et al. [97] looks at what they call "potentially intrusive practices", which includes privacy related practices such as behavioral profiling, reporting and analytics, targeted ads, identity and sign-in services, and fingerprinting. The studied users tended to want to opt-out of these practices, but generally resigned to trusting potentially misleading signals due to the difficulties of finding relevant settings.

A recent study by Mehrnezhad et al. [64] looks at the 100 top EU websites to study privacy-enhancing technologies, concluding that opting out of tracking—especially when you have previously opted in—is very difficult. How to opt-out varies greatly, and the most common ways offered are contacting service providers and changing browser settings, followed by initiatives for cookie information and opting out through third party websites.

Cookie descriptions, consenting and dark patterns: Santos et al. [94] showed that nearly 90% of cookie banners violated applicable laws, with majority of banners being vague in their purpose description. Other violations included deviations from freely given consent through the use of positive and negative framing, as well as absence of essential information necessary for an informed consent. An earlier study by Fouad et al. [36] supported this view, showing that 95% of cookies used on websites do not have an explicitly declared purpose.

Krisam et al. [56] examined and classified cookie disclaimers of popular websites in Germany and found over 85% to use dark patterns. Only a little bit over 20% of websites offered a one-click option for rejecting all cookies, thus not complying with the requirement of balanced choice. Machuletz and Böhme [60] shows that users tend to accept cookies to a greater extent

when the consent dialog uses dark patterns with a visibly default accept button, while at the same time being less able to recall this choice in comparison to control groups.

In the scope of dark patterns, Gray et al. [39] analyzes three types of consent banners from various perspectives, including legal. The study concludes that there is much to be done to combine design, law, ethics and more to prevent the use of dark patterns and empowering users. Habib et al. [41] also looks at various types and characteristics of consent banners, finding several dark patterns violating GDPR and CCPA such as unequal paths, bad defaults, confusing buttons, no choices and confirmshaming. Utz et al. [108] showed that 72% of users interacting with a consent notice did so because they were annoyed by it, and only 10% of the total participants interacted with it to protect their privacy.

Provider-based consent mechanisms: Violations of GDPR and other privacy legislation can easily spread with multi-site cookies such as TCF, where a recent study by Matte et al. [61] showed that a positive consent was stored in shared cookies for several websites even though the user had explicitly opted out. Another study by Matte et al. [62] shows that there are great variations in how advertisers use consent or legitimate interest as a basis for data processing, even for purposes that arguably should rely on consent. These studies shows both an abuse of TCF and a vulnerability of TCF in the sense that a single website can invalidate consent for the whole ecosystem.

Santos et al. [93] explores similar effects of less compliant CMPs, and additionally concludes that CMPs in many cases qualifies as data controllers, and thus should have an increased responsibility compared to what is required of a data processor.

Nouwens et al. [75] looks at dark patterns of CMP designs, finding that only 12% meet minimal requirements of European law, additionally confirming through user studies that dark patterns leads to increased consent.

Legislative compliance: Trevisan et al. [105] studied the impact of the ePD prior to GDPR and found that half of all visited websites violated the directive's requirement to obtain user consent before storing profiling cookies. As part of the study, a four-year comparison is made, where no significant difference in exposure to tracking technologies can be found.

Kretschmer et al.'s [55] study-of-studies reviews academic work of the impact of the GDPR on the web, concluding that even though GDPR has had an overall positive impact on privacy, there are still a lot of room for improvement when it comes to compliance. According to the study, a majority of policies still either lack required information or do not provide it in a user-friendly form and opting out is still to a large extent offered in inconvenient ways.

O'Connor et al. [76] takes a CCPA perspective and looks at the various ways websites offers opting out of sale. Like the case with studies of GDPR cookie banners, the use of deceptive designs to trick users into accepting default settings is common, even though this is not explicitly prohibited by CCPA. The study also finds and studies number of other inconvenience factors and how they affect user engagement.

Chen et al. [19] looks at privacy policies of popular websites in the light of CCPA, as well as surveys consumers regarding how they interpret the policies. The study shows that there are both vagueness and ambiguity from several perspectives: in CCPA, in privacy policies and in the interpretation of CCPA as well as privacy policies.

4.2 Recommendations for improving web privacy

Aside from evaluating the current state of web privacy, the aforementioned studies make several recommendations and suggestions. In this section we will briefly summarize the most commonly recurring categories to establish what improvements are most prevalent in research on web privacy.

Standardization: Several studies [19, 36, 91, 93, 94, 105] suggest more standardization and structure in the future to address issues including vagueness and ambiguity [19], easing language tensions [94] as well as having it be developed by a neutral party in contrast to content providers and similar parties [93]. Additionally, standardization can help with systematic and automatic auditing, as suggested in some studies [36, 93, 105].

Necessity distinction: There is a need for a clear distinction between necessary and unnecessary cookies, as pointed out in some studies [56, 94]. This can help with determining if some cookies should be rejected by default [94] and clarify what is really technically necessary from a legislative perspective [56]. A clear distinction would also help with standardized and automated auditing, as recommended in some aforementioned studies [36, 93, 105], to determine legal compliance.

Browser solution: Technical standardization and the use of privacy-preserving technologies to minimize the use of personal data are suggested by several studies [55, 91] especially concerning using standardized settings in browsers [41, 56, 76, 94, 97]. Browser settings is motivated by properties including neutrality and usability [97], and the fact that there is now legislation to support that kind of technical solution [41]—referring to the fact that previous initiatives have been considered as either ahead of their time or too simplified [60].

4.3 Legal requirements on browser-based consent mechanisms

Santos et al. [92] have made an extensive review of legislative requirements—primarily based on European legislation—and consent mechanisms on the web, presenting a list of 22 low-level requirements for valid consent through consent banner design. The requirements are categorized in seven high-level requirements: Prior, Free, Specific, Informed, Unambiguous, Readable and accessible, and Revocable. Table 4.1 presents all requirements of Santos et al. [92], with mapping of other studies mentioned in this thesis to the corresponding low-level requirement. Going forward, we will denote these requirements A1–A22.

Another categorization of legal requirements is presented in another study by Santos et al. [94], focusing on cookie banner text. The requirements are presented in Table 4.2, where we will denote the requirements B1–B6.

4.4 Properties of an ideal solution

Ideally, a solution should be serving both the data subject with privacy control, and the data controller with ensuring legal compliance. Based on the reviewed studies of current solutions, there is a need for:

- a more standardized and auditable approach to consent [19, 36, 91, 93, 94, 97, 105],
- a clear distinction between necessary and unnecessary cookies [56, 94], and
- technical enforcement of consent through browser mechanisms [41, 56, 76, 94, 97]

Combining the two sets of requirements from the work of Santos et al. [92, 94] with the additional suggestions above, we end up with a set of properties listed in Table 4.3, where property P1–P7 are based on consolidation of the legal requirements suggested by Santos et al. [92, 94] and properties P8–P10 are based on the identified suggestions in research of current solutions.

Table 4.1: Legal requirements on consent banner design and implementation by Santos et al. [92] with mapping to supporting research

Requirements		**Examples**
High-level	**Low-level**	**Previous work**
Prior	A1 Prior to storing an identifier	[61, 91, 92, 105]
	A2 Prior to sending an identifier	[91, 92, 105]
Free	A3 No merging into a contract	[92]
	A4 No tracking walls	[39, 92]
Specific	A5 Separate consent per purpose	[36, 61, 62, 92, 93, 94]
Informed	A6 Accessibility of information page	[76, 92]
	A7 Necessary information on browser-based tracking technology	[36, 92, 94]
	A8 Information on consent banner configuration	[92]
	A9 Information on the data controller	[92]
	A10 Information on rights	[92]
Unambiguous	A11 Affirmative action design	[41, 56, 61, 75, 91, 92]
	A12 Configurable banner	[39, 41, 56, 60, 61, 76, 91, 92]
	A13 Balanced choice	[39, 41, 56, 60, 61, 64, 75, 76, 92, 93]
	A14 Post-consent registration	[92]
	A15 Correct consent registration	[61, 92]
Readable and accessible	A16 Distinguishable	[76, 92]
	A17 Intelligible	[91, 92, 94]
	A18 Accessible	[39, 76, 92, 93]
	A19 Clear and plain language	[19, 36, 41, 92, 94]
	A20 No consent wall	[39, 55, 92]
Revocable	A21 Possible to change in the future	[41, 61, 64, 91, 92]
	A22 Delete ”consent cookie” and communicate to third parties	[64, 91, 92]

Table 4.2: Legal requirements on cookie banner text by Santos et al. [94]

Legal requirements	**Mapping to A1–22**
B1: Purpose explicitness	–
B1.1: Availability	A6
B1.2: Unambiguity	A19
B1.3: Shared common understanding	A17, A19
B2: Purpose specificity	A5, A19
B3: Intelligible consent	–
B3.1: Non-technical terms	A19
B3.2: Conciseness	A19
B4: Consent with clear and plain language	–
B4.1: Straightforward statements	A19
B4.2: Concreteness	A19
B5: Freely given consent	A3–4
B6: Informed consent	A7–10

Table 4.3: Proposed properties based on previous research

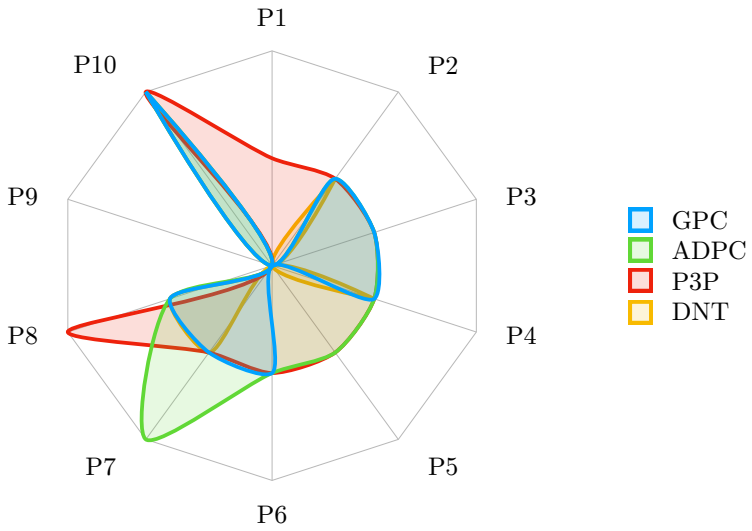
ID	Property	Description	Rationale
P1	No prior storing/sending	Consent must be obtained before storing and sending identifiers	A1–2
P2	Freely given consent	Consent should be voluntary, not merged into a contract and not forced with ”tracking walls” blocking access without consent	A3–4, B5
P3	Specific separate consent	Purposes should be precisely identified and defined, with consent given separately for each purpose	A5, B2
P4	Informed consent	Information should be available and accessible with necessary information on trackers, configuration, data controller and subject rights	A6–10, B1.1, B6
P5	Unambiguous consent	An affirmative, balanced configurable choice with correct consent registered no earlier than after given consent	A11–15
P6	Readable and accessible	Consent request should be clearly presented, unambiguous, understandable, accessible, simple and neutral. Consent request should be non-blocking (”consent wall”)	A16–20, B1.2–3, B2–4
P7	Changeable	Consent should be possible and easy to withdraw or edit, and revocations should result in cookie deletion and withdrawal from all affected additional parties	A21–22
P8	Standardized	Purposes should be standardized and based on legal requirements to prevent uncertainty and additionally allowing for auditing.	[19, 36, 91, 93, 94, 97, 105]
P9	No abuse of necessary	There should be a clear distinction between necessary and unnecessary cookies, where the latter should be rejected by default and subject to consent according to P1–8	[56, 94]
P10	Browser-controlled	Consent settings should be handled by the browser, with the browser signaling data subject’s choice to the data controller	[41, 56, 76, 94, 97]

5 Bridging the gaps

In this chapter, we will take a closer look at some browser-based consent mechanisms in order to first determine a candidate mechanism for improvements, and then review the identified properties with the selected mechanism in mind to suggest improvements.

5.1 Determining a browser-based consent mechanism foundation

With P10 pointing out a browser-based consent mechanism as the preferred choice for expressing consent, we return to P3P, DNT, GPC and ADPC to decide on a suitable foundation. Figure 5.1 shows a comparison of these mechanisms, with fulfillment of property P1–P10 (see Table 4.3) measured as fulfilled (full), partly fulfilled or implementation-dependent (half), or not fulfilled (none).



(The same data is alternatively presented in Table 5.1 below.)

Figure 5.1: Property fulfillment (fully/partly/none) of browser-based consent mechanisms.

As Figure 5.1 indicates, there is generally a low fulfillment of several properties, and there is not one single solution that is close to fulfilling all properties. With P3P and DNT being resigned or otherwise obsoleted, a continuation of those is not a feasible path. Instead, GPC and ADPC are the potential foundations for future improvements as they are currently in use either actively or in a prototype stage.

Similar to DNT, GPC has a narrower scope with the main purpose of sending (legally binding) signals to the data controller to prevent tracking or opting out of such. However, GPC have been considered ambiguous as publishers can treat the GPC signals differently, as well as the signals having different meanings in different jurisdictions. ADPC on the other hand aims at providing a broader privacy control, and measured against the identified properties it fulfills more of them than GPC does.

Even though ADPC still either partly or fully lacks in fulfillment of many properties, we can conclude that it provides the best fulfillment of current browser-based consent mechanisms and as such can be determined to be a suitable foundation for improvements, aiming to bridge the gap and fulfill the remaining properties.

Table 5.1: Gaps of browser-based consent mechanisms and effect of potential improvements

Mechanism	Status	*No prior storing/sending* **(P1)**	*Freely given consent* **(P2)**	*Specific separate consent* **(P3)**	*Informed consent* **(P4)**	*Unambiguous consent* **(P5)**	*Readable and accessible* **(P6)**	*Changeable* **(P7)**	*Standardized* **(P8)**	*No abuse of necessary* **(P9)**	*Browser-controlled* **(P10)**
P3P†	Retired	◐	◐	◐	◐	◐	◐	◐	●	○	●
DNT†	Unsupported	○	◐	○	◐	○	○	◐	◐	○	●
GPC*	Draft/Active	○	◐	◐	◐	○	◐	◐	◐	○	●
ADPC*	Draft/Prototype	○	◐	◐	◐	◐	◐	◐	◐	○	●
ADPC enhancement	*(suggestions)*	●	◐	●	●	●	◐	●	◐	●	●
Data controllers	*(requirements)*	–	●	–	–	–	●	–	–	–	–
Legislation	*(potential)*	–	–	–	–	–	–	–	●	●	–
Combined effect of above	–	●	●	●	●	●	●	●	●	●	●

● = fulfills property; ◐ = partly fulfills property or usage-dependent;
○ = does not fulfill property; – = not applicable

† = W3C official standard; * = unofficial draft

5.2 Current state overview

Table 5.1 describes an overview of each browser-based consent mechanism measured on the identified properties, as well as the potential effect of adding improvements to ADPC (which will be presented in the remainder of this chapter), requirements from data controllers and potential legislation. The last row shows the combined effect of all.

To further explore the gaps of each property, the following section will review each property from an ADPC perspective and highlight the main takeaways required for the suggested improvements. Note that in some cases, the potential fulfillment is not notably improved in terms of property fulfillment (partly fulfilled both as current and potential, for instance), but

this is still an improvement over the current state even though it is not enough to fully fulfill the property.

5.3 Review of properties and suggestions for improvement

With ADPC being identified as the platform to improve on, let us evaluate in which ways features need to be added or enhanced to the current ADPC draft[1] in order to fulfill as many of the identified properties as possible. For each property, we will describe the requirement and suggest improvements that can help fulfill the property.

No prior storing/sending (P1) Browsers should prevent or limit storing and sending data unless there is a registered consent. Either configured by the user to allow generally, or a specific consent per website. This goes for both storing and sending.

No prior storing/sending (P1)	
Fulfillment	○ Current ● Potential
Requirement	Browsers should only accept to store data on and sending data from a client side if there is a registered specific consent configured by the data subject or stated as necessary by legitimate interest (see P9).
Suggested improvements	• Add browser support for ensuring prior consent

Freely given consent (P2) Keeping consent within the browser prevents consent from being merged into a contract. Any other contract is not allowed to overrule the usage agreed through consent settings. The website is not allowed to block access or hinder it in any way to force the user into consenting to certain data sharing.

Freely given consent (P2)	
Fulfillment	◐ Current ◐ Potential
Requirement	Consent control in the browser ensures consent outside contracts. Websites are obliged to not force a consent through ”tracking walls” forcing the user to give consent.
Suggested improvements	• Add browser support for expressing consent • Add browser/server support for consent withdrawal • Prohibit the use of tracking or consent walls

Specific separate consent (P3) All consent needs to be given specifically and precisely per purpose. No bundling of purposes or general consent requests should be allowed to use. This is handled through browser settings.

[1] `https://www.dataprotectioncontrol.org/spec/`

Specific separate consent (P3)	
Fulfillment	◐ Current ● Potential
Requirement	Consent control should be granular, purpose-specific, and not allowed to be expressed in general or bundled purposes.
Suggested improvements	• Add browser support for granular consent control

Informed consent (P4) Privacy information should be easily accessible; including ADPC support within the browser interface in a standardized way would be one way to comply with this. The required information would be up to the data controller to provide, and for ADPC/browser to enforce. All cookies should be documented, and as such the browser could prevent usage of undocumented cookies. Preventing data controllers from having nonsense documentation would be up to auditing instead of browsers. Information on the data controller and user rights should also be available for each website.

Informed consent (P4)	
Fulfillment	◐ Current ● Potential
Requirement	Information required for informed consent should be enforced technically by blocking undocumented cookies and/or alert the user if data is missing.
Suggested improvements	• Add browser support for fetching and controlling consent information

Unambiguous consent (P5) Consent should be clearly given, and as such implementations should not allow for ”approve all” or default consent. This is important as the default-DNT is credited as one main reason that DNT did not succeed. The browser should support granular configuration and manual approving/consenting to each usage. In combination with P1, the browser ensures that the consent is correctly registered, accepted and enforced.

Unambiguous consent (P5)	
Fulfillment	◐ Current ● Potential
Requirement	Granular consent configuration in a standardized interface ensures fulfillment of non-unambiguous consent.
Suggested improvements	• Design browser consent interface so that no ”allow all” or similar is used

Readable and accessible (P6) Consent information should be readable and accessible, and browser implementation ensures that the information is consistently found through the interface. This also ensures that there should not be any ”consent wall” blocking the interface of the website. The intelligibility and use of clear and plain language is more challenging for the browser to ensure, and as such is up to the data controller to provide. Standardizing where the data controller provides this data also opens up for easy auditing of information, for instance through Flesch-Kincaid test[2] to enable automation.

[2]The Flesch–Kincaid readability tests are used to determine reading ease by word and sentence lengths.

Readable and accessible (P6)	
Fulfillment	◐ Current ◐ Potential
Requirement	The browser implementation should enable the data controller to provide the correct information, but the data controller is still in charge of what to provide.
Suggested improvements	• Add browser support for retrieving consent information from a well-known location

Changeable (P7) ADPC fully supports the possibility to change (giving and withdrawing) consent, even as a stand-alone request through an HTTP `HEAD` request. However, there is no standardized response and thus no way of knowing if this request has been processed and/or accepted. Potentially a new privacy request, `PRIVACY` or similar, could be introduced to ensure that the request is handled in a prioritized way and with a standardized response format. First-party withdrawal might be more trivial than third-party withdrawal, but that is up to the data controller to solve as it is a choice of responsibility when utilizing third-party data exchange.

Changeable (P7)	
Fulfillment	◐ Current ● Potential
Requirement	Withdrawal of consent, and potentially other consent changes, should have a standardized response to confirm that action has been taken on the withdrawal.
Suggested improvements	• Add browser and server support for consent withdrawal, utilizing the same interface as for consent

Standardized (P8) In its current draft, ADPC only specifies one standardized personal data identifier: `direct-marketing`. It is called an ”objection identifier” and is used to communicate what personal data processing the user objects to. This is still an open-ended part of the ADPC standard, and a gap where legislation and data protection authorities need to define a standardized taxonomy to be used. This can also help facilitate scalable auditing.

Another perspective on standardization is how descriptions of and information on cookies, data controller, rights, etc. should be structured and made available. This is something that is currently not solved in ADPC even though it gives some flexibility. In order for browsers to easily locate the information needed, a standardized path using a well-known URI as well as an expansion of the ADPC consent structure to include information on cookies, data controller, rights, etc. would help fulfill the standardization property.

Standardized (P8)	
Fulfillment	◐ Current ◐ Potential
Requirement	Location of required information needs to be standardized, and the structure for information included should be expanded to include all information that the other properties require. Purpose taxonomy is a subject for future work from a legal perspective.
Suggested improvements	• Standardize locations for data and protocols for communication

No abuse of necessary (P9) Cookies can be allowed without any consent as long as they adhere to the requirement of legitimate interest. There is a fine balance to be made here, as data controllers should not misuse this property to put everything under legitimate interest. Similar to P8, further clarification can be of need from a legal standpoint, but to a large extent GDPR is already clear on what is included in legitimate interest. In order to support transparency, all cookies should be motivated and explained—even those considered to be necessary and to be allowed based on legitimate interest. By utilizing the same standardized approach as P8 suggest, necessary cookies can include a `necessary` attribute and be allowed to be used pre-approved only by making sure that all data is complete. This would allow for broad scale auditing of websites to reveal any misuse of trust and thus possible to black-list or similar. Examples of necessary cookies would be settings (language, layout, dark mode, etc.) as well as active log-in action to keep session alive. Necessary would always be session cookies unless the user actively (not pre-selected) confirms with a checkbox to remember the settings for a defined period of time.

No abuse of necessary (P9)	
Fulfillment	○ Current ● Potential
Requirement	Cookie definition should include a `necessary` attribute or similar to define that it is necessary and acceptable under legitimate interest. The cookie is allowed to be persistent if and only if the user actively consents to that.
Suggested improvements	• Add browser support for allowing correctly specified necessary cookies

Browser-controlled (P10) GDPR name technical setting as a way of expressing consent [85, Rec. 32], which suggests that ADPC can be integrated into the browser with easy-access consent configuration. The WP29 has written expensively about requirement for consent, and in this naming browser settings as a way to obtain consent [87]. The data controller must be *"confident that the user has been fully informed and actively configured their browser or other application"* [87, p. 4]. Additionally, it should not be possible to bypass choices made by the user, and the browser should in cooperation with other parties *"convey clear, comprehensive and fully visible information in order to ensure that consent is fully informed"* [86, p. 15]. WP29 notes that it is important that browsers are provided with default privacy-protective settings, adding that browsers should have privacy wizards upon first install/update that requires users to express their choice.

Browser-controlled (P10)	
Fulfillment	● Current ● Potential
Requirement	Browser settings are required to provide clear, comprehensive, and fully visible information to ensure informed consent. The settings should be easy to access and the consent not possible to bypass. WP29 recommends to us default privacy-protective settings, as well as having a privacy wizard to help users express their choice.
Suggested improvements	• Implement browser support with both interface and browser engine according to the suggestions of P1-9

6 Putting it all together

In this chapter, we will suggest how ADPC can be improved, implemented, and put to use. The following sections will review the involvement of all parties—namely browsers, server software and data controllers—and propose an implementation roadmap with division of responsibilities between these parties. Going forward, the improved version of ADPC will be denoted ADPC+.

6.1 Suggested features

In this section we will condense the suggestions from each property in the previous chapter into distinct features that can be implemented. For each feature, we will present what is included and what stakeholders are responsible for implementing and/or providing information in order for the feature to fulfill the intended properties. Even though these features are presented as enhancements to ADPC, it would be possible to implement them as stand-alone features or as a new standard.

6.1.1 Feature 1: No prior storing/sending of data

This feature primarily fulfills P1 and are implemented in the browser. Browsers should only accept storing and sending cookie data and similar if there is a registered specific (per website, cookie, purpose) consent configured by the user (handled by Feature 2). The only expectation to this rule is necessary cookies, as specified in Feature 5 according to P9.

Browser software	✓ Implement blocking of storing/sending data prior to consent.
Server software	–
Data controllers	–

6.1.2 Feature 2: Present complete and required information

This feature is a shared responsibility between the browser software and the data controllers. Browsers provide a standardized interface that is populated with data from the data controller. When a user visits a website, the browser loads the information from the server and displays

it in the dedicated interface and notifies the user. As an effect of this, there should not be any tracking or consent walls; however, this requires that data controllers respect this and should be a requirement for complying with ADPC+.

All information required from the data controller should be located on a well-known location such as `/.well-known/privacy` or `/.well-known/adpc` with a minimum of two files: one with information on the data controller and the user's rights, and one with information on all cookies including their associated usage, consent request, and motivation. The main file should include a list of languages that the information is available in, which then could be located using an ISO country–language standard suffix, i.e., sv_SE.

Cookie information should include a general explanation of the cookie, what it contains, tracks or is used for. As a basis for giving/withdrawing consent, the purpose(s) of why the information is requested should be clear, with one explanation per purpose. If the cookie is necessary (see Feature 5), shared with third parties, or persistent, the purpose of this should be motivated specifically within a `necessary`, `shared`, and `persistent` attribute, respectively. The persistent motivation should include and motivate the cookie's lifetime.

The information provided should be easy to read: intelligible with a clear, plain, and generally understandable language. Multi-language support is already available in ADPC, and supporting all applicable languages based on target audience is recommended. Auditing can be made through Flesch–Kincaid tests or similar.

Browser software	✓ Implement an interface for presenting privacy and consent data. ✓ Fetch data by querying a well-known location upon each of the user's first-time domain visit.
Server software	–
Data controllers	✓ Provide all the required privacy, consent, and cookie information in the given well-known location. ✓ Ensure the language is clear, plain, and generally understandable. Preferably in all target-audience languages.

6.1.3 Feature 3: Configurable and changeable specific separate consent

This is the key feature and heart of a browser-based consent mechanism. It should be configurable (P5) and changeable (P7), and it needs to handle consent separately for each purpose (P3). The browser is responsible for providing this interface, and it can preferably be combined with the interface of Feature 2 to ensure specific (P3) and informed (P4) consent. In combination, this helps prevent tracking and consent walls as noted in Feature 2.

Consent should be given by confirming each cookie–purpose pair through an affirmative action, such as checking a checkbox and saving the configuration. No "allow all" or similar should be possible unless it concerns withdrawal or unchecking.

Third-party cookies should be controlled in the same way as first-party cookies but can be specifically marked. The data controller is responsible for ensuring that third parties comply with ADPC+.

In the event that a change leads to withdrawal of consent, the browser should immediately communicate this to the data controller's server. If the withdrawal concerns a third party, the data controller is responsible for ensuring withdrawal and should inform the browser when the withdrawal is confirmed. The browser may try to withdraw the third-party consent as well but is not responsible for doing more than signaling the first party data controller. Signaling is further described as Feature 4.

Browser software	✓ Implement an interface for giving and withdrawing consent, in connection with information in Feature 2. ✓ Use signaling to send and monitor consent withdrawal.
Server software	✓ Implement support for consent withdrawal and forwarding.
Data controllers	✓ Ensure all consent withdrawals are correctly handled. ✓ Do not utilize tracking or consent walls.

6.1.4 Feature 4: Browser–server and server–server communication

In order to support Feature 3 and possible other future features, a communication protocol for browser–server and server–server communication must be established. Of central importance is the possibility to communicate, respond to and forward consent withdrawal. Additionally, a method for nudging the user and/or asking for additional consent could help appease data controllers.

An `ADPC` header is already used in the current ADPC draft, including for withdrawing consent; expanding on this would be the preferable choice. Aside from handling a consent withdrawal locally, a server should be able to forward third-party consent withdrawal to the intended party and ensure the withdrawal is confirmed. The responsibility for this ultimately lies in the hands of the data controller, but automated methods is important to ensure the withdrawal. When a withdrawal is confirmed, a confirmation should be returned to the initiating browser.

If a website for any reason wants to ask for additional consent (on a non-frequent basis), the server could include a review request in the `ADPC` header field of an HTTP response. A message explaining the request could potentially be included to nudge the user with or display in the consent interface. A limitation to only allow such nudges on a daily, weekly, or similar basis can be allowed in the implementation. In more blocking cases, it could be possible to establish certain HTTP status codes such as `2xx`, `3xx` or `4xx` to indicate limited, redirected, or unavailable, respectively, based on limited consent settings. The same would also be possible to communicate without HTTP status codes through the custom header instead.

ADPC message compliance should be possible to check, for instance through querying a server with the `OPTIONS` method using the `ADPC` header field, to which the server should respond with a confirming response. Aside from using the `ADPC` header field, it is also a possibility to introduce new privacy headers and/or use other HTTP methods such as `POST` or `PUT` depending on server support.

Browser software	✓ Implement support for ADPC header fields. ✓ Implement support for sending/retrieving consent requests.
Server software	✓ Implement support for ADPC header fields. ✓ Implement support for sending/retrieving consent requests.
Data controllers	–

6.1.5 Feature 5: Require consent for cookies without `Necessary` attribute

This last feature aims at satisfying P9 by preventing abuse of calling certain cookies necessary based on legitimate interest. The idea is that the data controller explicitly needs to classify data and purposes as necessary and specify this in the information provided through Feature 2. This not only requires a cookie to be classified as necessary; it requires a motivation why. As necessary cookies do not require consent, this increases the demands of classifying cookies

as necessary. Browsers should only accept cookies as necessary if they are stated as so and motivated according to Feature 2.

The data controller should provide information on the cookie with a `necessary` attribute motivating the classification with legitimate interest per purpose. Note that necessary cookies are required to be first party, and thus third-party cookies classified as necessary will be blocked or subject to consent.

Examples of necessary cookies and purposes include, but are not limited to; user session data, authentication, security, streaming/network management, preferences, etc. By requiring each of these to be both classified and marked, it allows for semi-automated auditing where servers can be queried to retrieve a list of necessary cookies and purposes that can be reviewed.

Browser software	✓ Implement support for determining necessary cookies and uses. ✓ Only allow correct necessary cookies without consent.
Server software	–
Data controllers	✓ Provide complete information according to Feature 2 on all necessary cookies. ✓ Do not abuse the use of necessary—it is legally enforceable.

6.2 Incentives and effects on affected parties

6.2.1 Technical implementers

In the age of GDPR and CCPA, user privacy is a competitive advantage. Not only are an increasing number of privacy-aware users looking for applications that value their privacy, but legislation is also working towards protecting even the not-so-privacy-aware users as well. The initiatives already taken by major browsers shows that privacy is on the agenda.

If a browser could offer an alternative to cookie banners that would both unify the consent mechanism in-browser as well as adding additional protective features based on those to limit data sharing, this would be an enormous benefit for the user and a strong case for possibly switching browser to a more privacy-aware one.

For servers, the incentive boils down to being compliant with web standards—which ADPC+ would potentially be qualified for. In the meantime, plugins for ADPC+ server support could be developed that website owners and data controllers can choose to utilize, which would create an incentive for server providers to use plugins until native support is offered by the server software vendors.

6.2.2 Data controllers

One notable effect of the suggested features is an, at least potentially, increased burden on data controllers. However, some if not all of what needs to be done have already been done by compliant data controllers but through other mechanisms. Over time, applications and services aimed at ADPC+ will help simplify the amount of work required by data controller to provide the requested information.

From an incentive perspective, legal compliance might be the most prominent one. The potential economic blow of being fined for GDPR noncompliance and breaches is a strong motivator by itself. There are of course also data controllers that are self-motivated to show strong respect for user privacy and thus would have ADPC+ compliance as an incentive in itself to showcase this.

With more privacy awareness, data subjects might be more likely to choose websites that respect user privacy in the future. This potential is also an incentive towards complying with ADPC+ for showcasing respect of user privacy.

6.2.3 Data subjects

Finally, the reason all privacy legislation has been established: data subjects. Needless to say, the effect on data subjects is of central importance in the suggested improvements and the primary reason for why they are at all needed. Complete implementation of the suggested features would create a notably enhanced user privacy and data control, as well as creating strong incentives for data controllers to comply—effectively creating a positive snowball effect of user privacy enhancement.

Having to almost unavoidably configure settings in the browser might come off as a worsened user experience to some, especially those who have utilized content blockers before to remove privacy notices and cookie banners. However, this is a small price to pay in order to increase the user privacy, and also a necessary one in order for data controllers to be able to depend on valid user consent. A unified experience, both out-of-the-box and as a platform for future improvements, would ultimately improve the user experience and decrease the cookie banner configuration-overhead of today.

6.3 Implementation roadmap

Implementation of the proposed features would have to begin with adding the features to the existing ADPC standard. Once the features have been standardized, browsers and server software can implement support for ADPC+ in order for data controllers to use them. It is only when data controllers provide the required information and make use of the implemented features that the data subject can benefit from them through their browser experience. Figure 6.1 illustrates the dependencies and influences in the suggested implementation process.

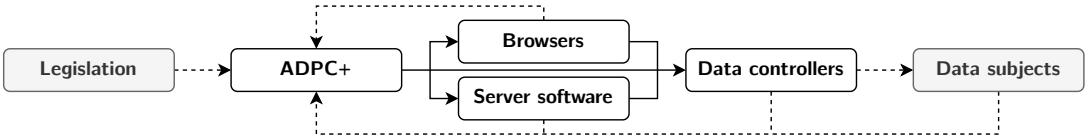


Figure 6.1: Implementation dependencies and influences

Even though legislation is clearly the driver here, the suggested features are based on the current European legislative landscape and explains why the implementation process starts with ADPC+. However, going forward the foundation for enhancements to ADPC will be legislation as well as feedback from browsers, server software, data controllers, and data subjects.

The initial work would have to define the standard, based on the proposed solution. Initially, this would be a work involving the ADPC community to sketch out an enhanced draft. In order for the enhanced ADPC to reach a broader audience and a broadly accepted standard, standardization bodies such as World Wide Web Consortium (W3C) and Internet Engineering Task Force (IETF) would need to be involved. No matter the scenario, documentation of the ADPC enhancements will need to be the first step before other stakeholder can start with the remaining work.

Table 6.1 at the end of this chapter shows an overview of the division of responsibility derived from the proposed features. Once the updated ADPC standardization is finalized, implementation of the features can begin. The proposed features of ADPC+ are all dependent on browser implementations, and there are two ways to do achieve this: One is the current (prototype) variant, meaning creating plugins to browsers adding the needed functionality. The other one is the preferred one, where the functionality is instead implemented by the browser vendor as part of the browser offering. Both the browser user interface and the browser engine would need to implement features in order to fulfill the requirements. The latter would need to be developed alongside the server software in order to ensure compliance.

Server support is required to enable browser–server and server–server communication, especially used for consent withdrawal and other privacy related communication. Like in the case of browsers, plugins, or native support for server software like Nginx and Apache need to be developed for these features. Compatibility with browsers engine capabilities is crucial to ensure support.

Data controllers are ultimately responsible both for using the server implementations, and to provide the information required for the browser functionality and legal compliance. ADPC+ will provide the framework of being compliant, but in the end, data controllers will be responsible for complying with what the features requests in order to stay legally compliant.

6.3.1 Incremental deployment

Based on responsible parties for different features, it is possible to incrementally deploy the suggested features. However, many features depend on other features so functionality might need to be tweaked in order for them to be implemented individually.

Figure 6.2 shows the feature dependencies. Feature 1 is dependent on having valid consent data, offered by Feature 3, and consent exceptions, offered by Feature 5. Feature 3 is dependent on having required information, offered by Feature 2, and withdrawing consent through browser–server and server–server communication, offered by Feature 4. Feature 5 is dependent on Feature 2 to provide functionality for `necessary`.

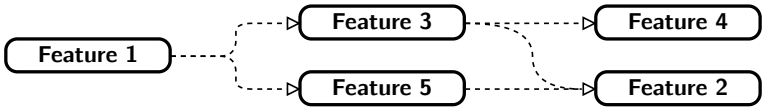


Figure 6.2: Feature dependencies

What we see here is that Feature 2 and 4 are not dependent on any other features. Feature 2 relies on data controllers to provide the requested information and browsers to provide a user interface for displaying the information. Feature 4 relies on browsers and servers to implement support for communication. Hence, Feature 2 and 4 are possible first features that could be used independently, with Feature 2 being the most usable as it provides information to the end-user.

That being said, the idea with ADPC as of today—and the suggested features—is that it can be incrementally developed and deployed. Nevertheless, a constant alteration of documentation and standards that set a framework is not desirable, so in order to create an environment for compliance, a cohesive, coordinated, and synchronized implementation between all parties is strongly preferable.

6.4 Evaluation of property fulfillment

With the presented features, ADPC+ bridges the gaps of several properties, as showcased as possible in the gap analysis. Table 6.1 shows all features and maps how they contribute to each property, as well as a summarizing property fulfillment of the combined ADPC+. Together with legislation and data controller compliance, this solution comes very close to an ideal solution as mapped out by the identified properties.

In Appendix A.1, there are some additional feature ideas that could provide even more value but are outside the scope of requirements from the suggested properties.

Table 6.1: Suggested features, implementation responsibility and property fulfillment

Features	Implementation							Property fulfillment										
ADPC feature additions	*No prior storing/sending*	*Freely given consent* **(P1)**	*Specific separate consent* **(P2)**	*Informed consent* **(P3)**	*Unambiguous consent* **(P4)**	*Readable and accessible* **(P5)**	*Changeable* **(P6)**	*Standardized* **(P7)**	*No abuse of necessary* **(P8)**	*Browser-controlled* **(P9)**	*Data controller*	*Server support*	*Browser support*	**(P1)**	**(P2)**	**(P3)**	**(P4)**	**(P5)**	**(P6)**	**(P7)**	**(P8)**	**(P9)**	**(P10)**
F1: No prior storing/sending of data	×			✓		✓				✓				✓								✓	✓
F2: Present complete and required information	×		×		✓		✓									✓							✓
F3: Configurable and changeable specific consent per cookie and purpose	×	×	×		✓		✓		✓							✓			✓				✓
F4: Browser–server and server–server communication	×	×																		✓	✓		✓
F5: Require consent for cookies without `Necessary` attribute	×		×																			✓	✓
Resulting property fulfillment				●	◐	●	●	●	◐	●	◐	●	◐										

× = party responsible for feature; ✓ = property contributed to by feature

● = fulfills property; ◐ = partly fulfills property or usage-dependent; ○ = does not fulfill property

7 Discussion

7.1 Results

Setting out to solve the challenges of privacy online is a bold under-taking, but an important one too. Creating an ideal solution is all but easy, and the suggested solution in this thesis is designed as an expansion of a recently proposed draft of ADPC. The suggested features can be implemented as stand-alone features outside of ADPC but given the history of failed initiatives in the privacy domain, cooperating to create a unified standard might be a better approach. ADPC has only been around for a year, and only on a prototype stage. However, based on the reviewed research, it is clear that the breadth of ADPC is beneficial and desirable from a user privacy perspective compared to narrower mechanisms such as DNT and GPC.

The result can be considered to be presented in three distinct parts and stages:

1. a set of properties derived from legal requirements and research suggestions (Chapter 4)
2. a formulation of requirements for browser-based consent mechanisms (Chapter 5)
3. a set of suggested concrete features building on ADPC, including implementation roadmap, dependencies, and responsibilities per stakeholder (Chapter 6)

From the reviewed research, it is surprising to see how bad the current state of privacy control really is. On one hand, it is a cat-and-mouse game with legislative demands and slow-moving technical initiatives; but on the other hand, it is a poorly synchronized cooperation where previous technical initiatives like P3P and DNT have been obsoleted—most possible due to lack of legislative support. Given the increased legislative demands, the time is definitely right to propose web privacy standards that can gain legislative support, as GPC already has.

The proposed solution, with suggested features, is based entirely on properties derived from research. The properties are based both on technical–legal requirements and recurring recommendations regarding privacy and consent mechanisms. The aim is that the presented properties can provide support for similar appliances in the privacy domain.

The actual implementation is outside the scope of this thesis but is a natural suggestion for future work. Implementing a working prototype would have been a larger and more technically demanding undertaking, requiring development of both browser and server plugins. This work has instead been primarily research-based, in order to provide a well-motivated foundation for suggested features.

Worth noting in the presented solution is that it puts emphasize on the client side rather than the server side, thus potentially helping with implementation as the incentives are larger on the client side and overhead on the server side is best avoided. The main driver—aside from client demands—is legislation, which also works as a motivator for data controllers to provide the required information and request the functionality from server software and browsers. Furthermore, the solution is relatively lightweight, building on existing web standards and principles, with the only main source of overhead being the requirement to serve consent withdrawals.

The resulting features are suggested as enhancement to ADPC in order to utilize an existing foundation. The result could however be implemented as stand-alone features, as part of another protocol, or as part of a new protocol with the suggested set of features. In the case of not using an existing protocol, additional work would be needed to create the foundation of the protocol, establishing ways of communicating etc. This is a possibility that can be considered as part of expanding on this work.

7.1.1 Limitations

There are some limitations to the provided solution. Most notably, it depends on a fairly recent and untested prototype of a privacy protocol. The ideas are however general, and even without ADPC as a foundation they would be possible to implement with a little tweaking and a more extensive work with supporting documentation.

Furthermore, the implementation relies on browser vendors and server software to implement support before even allowing data controllers to supply the information needed for compliance. Even if the ideal solution relies on official implementation by browser vendors and server software, it is possible to create plugins similar to the current prototype of ADPC.

The suggested features do not fully solve P9 (Standardization). It does solve the technical standardization, but more guidance is needed from legislation in terms of pre-defined purposes and similar. The features cannot fully ensure P2 (Freely given consent) and P6 (Readable and accessible) either, as there are still ways for data controllers to force users in to give consent and to provide incomplete or otherwise non-compliant information. These limitations are best mitigated through auditing, which has also been suggested by research.

7.2 Method

The method consisted of several parts: First, an extensive literature search and review, identifying relevant work with an academic breadth. Second, a combination and condensation of findings in the aforementioned research to present a set of properties for which technical solutions could be compared to. Third, a benchmark and gap analysis of identified browser-based consent mechanisms against the derived properties and a presentation of suggested improvements. Fourth, and lastly, a presentation of suggested features with an implementation roadmap and an evaluation of the resulting fulfillment.

If the study was to be repeated, more emphasis could have been put on the evaluation of browser-based consent mechanisms and adding a protocol for how property fulfillment was assessed. Another possibility would be to add actual testing of the identified mechanisms instead of only doing a theoretical comparison. Ideally, a working prototype of the proposed features could have been implemented but was decided to be outside of the scope of this thesis as stated in the delimitations.

7.2.1 Replicability

The work of this thesis has been structured as presented in Chapter 3. The study can be repeated through the method structure and description, but some parts such as ways of identifying relevant research, how to assess fulfillment, and some other similar areas are not described

in close detail and thus might differ in a repeated study. The overall structure is however possible to re-use as a method for a repeated study.

7.2.2 Reliability

Given that finding and reviewing relevant research is manual qualitative work, there is a possibility that a similar effort would yield a different result. However, based on what have been identified in research it seems that the user-privacy field circles around similar topics and challenges, suggesting that a repeated study would have several touching points with this study. However, the suggested features and how the properties were combined is something that could be varied, and a final solution might look very different even though it is closely related.

7.2.3 Validity

Given the qualitative nature of this work and strong reliance on previous work, validity has been of high importance in this work. Most prominent is the validation of the extensive legal–technical work by Santos et al. [92, 94], which constitutes a significant portion of the foundation in this thesis. In order to strengthen this foundation and validate the requirements, each requirement has been mapped to previous work identified through the research review.

7.2.4 Source criticism

The work with this thesis began with an extensive search for sources. Primarily, the bibliography consists of papers from proceedings of reputed conferences, as well as standardization and legislative bodies. Other web sources have been used sparingly, primarily to provide some additional perspectives or support, and never as a vital foundation for the continued work.

7.3 The work in a wider context

The motivation behind this entire thesis lies within the web-societal aspects of privacy regulations, legal compliance, and technical solutions to these challenges. The cookie banner has become the annoying symbol of user privacy legislation, and hopefully this work can contribute to a less annoying and more ethical privacy data environment tomorrow.

7.3.1 A note on ethical considerations

Even though the work with this thesis did not run in to any ethical considerations as far as the thesis work extends, there are several ethical considerations that have had to be made in the research work that this thesis refers to. Especially, user studies evaluating effects of different consent banner designs, understanding of technical concepts and terminology, etc., do need to consider ethical aspects. Research based on user studies have done some of the following: study reviewed and approved by university ethical review boards, made sure to comply with legal requirements, used opt-in for participation, offered drop out at any time, minimized data collection, used data anonymization, and more.

Another take on ethical aspect is what the result of this thesis seeks to address: Preventing the use of unethical consent influences, dark patterns, etc. With this perspective, the result of this thesis suggests features that strengthen data subjects online by preventing and mitigating unethical and undisclosed data usage.

8 Related work

From the extensive literature search, a broad range of related research have been identified. Some are more closely related to the scope of this thesis, and some are more loosely related.

Online user privacy

There have been several studies of user tracking in more unethical domain such as browser fingerprinting, mobile tracking and similar. Papadogiannakis et al. [78] looks at how websites bypasses GDPR consent, concluding that 75% of tracking activities happens before users can give consent or chooses to reject. Pugliese et al. [90] studies users' perspectives on fingerprinting and how to protect themselves. As new protocols arise, fingerprinting might—at least temporarily—be more challenging, as showcased by Smith et al. [96] that looks at fingerprinting of QUIC with TCP-trained classifiers. Other related work includes formal models of data sharing [104] and comparisons of web tracking on mobile and desktop environments [111], the latter showing a notable difference with mobile tracking having a potentially more severe impact. User awareness, adoption to, and misconceptions of web privacy tools is also an interesting and closely related area that has been studied [99].

Privacy notices is a central concept, and some studies have already been mentioned in the main text. Additional perspectives are how privacy can be enhanced through design [52], and additional effects after GDPR [59]. One emerging trend of recent years is to use machine learning for interpreting privacy policies [4, 13, 49].

Technical standard for CCPA have had a few studies conducted [43, 76, 113], and legal effects of GDPR was studied even before the final version of GDPR was approved [14]. There are also more dimensions of online privacy than cookies; one such example being a proposal to enhance privacy for TLS over TCP Fast Open [101].

Undisclosed and non-web tracking

Tracking in apps is also an emerging area of interest. Han et al. [42] compares the privacy in free and paid apps, finding that paid apps to a large extent use the same third-party libraries and permissions as their free counterparts, contrary to user exceptions. Kollnig et al. [54] show that most apps use third-party tracking, but only a few obtained valid consent before. There has also been initiatives to find universal guidelines of how to display and use consent

dialogs [29]. Another related domain is privacy in Internet of Things where access control policies and privacy preference languages have been proposed [6, 106]. Privacy policies have been extensively studied and proposed in areas also outside of the web, such as for health and other more general appliances [25, 40, 63].

From a developer perspective, there has been studies both on specifically nudging developers about user privacy [102], and development of privacy design patterns based on privacy principles and UML [100].

Policy languages

There have been many initiatives within the area of consent, transparency, and privacy, with several policy languages presented [9, 48, 51, 68, 112] and initiatives to enforce them [1]. Similar to the legal foundation in this thesis, there has been previous research in the interdisciplinary legal–technical domain seeking to technically bridge legal challenges [58]. Additional proposals have also been presented in the light of GDPR [8, 38].

The policy-aware web is a notable initiative, aimed at creating a rule-based policy management system and building on the semantic web [109, 110]. A recent example seeks to create a systematization of longitudinal privacy management [95].

9 Conclusion

In this thesis, we have explored the domain of user privacy and consent control, aiming to present a proposal for usable privacy features where the user is put in control. The result of this work is a proposed a set of features for browser-based consent mechanisms, arguing based on research that user consent could indeed be expressed through browser settings and comply with legal requirements.

As part of providing this result, we have answered the following research questions:

1. **What are the current challenges and requirements of user privacy control online?**
   This thesis has identified the current challenges and requirements of user privacy control online, presented in Chapter 4 with a proposed set of properties based on research. Expanding on previous work, this thesis identifies standardization, distinction of necessary and unnecessary cookies, and technical enforcement of consent through browser mechanisms as additional properties of an ideal solution.

2. **How can browser-based consent mechanisms provide conditions for legal compliance?**
   This thesis has suggested how browser-based consent mechanisms can provide conditions for legal compliance. Motivated by GDPR and WP29, as presented in Chapter 5, the suggested features showcase how valid consent can be expressed through browser-settings and thus provide conditions for legal compliance.

3. **What features of a browser-based consent mechanism are required to bridge current gaps, and what are the steps needed to implement them?**
   This thesis has presented features of a browser-based consent mechanism that bridge current gaps, as well as presented a roadmap of what steps are needed to implement them—all found in Chapter 6.

The result of this work can be implemented in many different ways. Ideally, the features are implemented into ADPC as proposed, with browsers and server software picking up on the ideas and implementing support. In the meantime, a prototype implementation to use as a proof-of-concept is the natural next step suggested as future work. The features can also, as discussed in previous chapters, be implemented as stand-alone features, as enhancements

to other protocols, or as a new protocol including the suggested set of features. This too is considerations for future work.

Returning to the specification of the `Comment` field in the 1997 cookie standard, this proposal—presented 25 years later—might finally allow for fulfilling that same intention: enabling informed consent and allowing users to decide whether to allow a cookie or not. That being said, let us see what the coming 25 years have in store..

9.1 Further studies

There are numerous paths to go from the work presented in this thesis. First and foremost, implementing the suggested features based on ADPC is the natural next step based on the presented result. It could be either implemented with the full feature set, or with stand-alone features as suggested in the implementation roadmap. Prototype plugins would allow for the features to reach a broader audience.

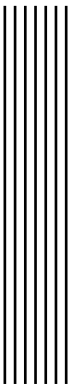
Another expansion of this work would be to include more legislation: CCPA, LGPD, PDP, CPPA, and more. A technical solution would probably benefit from relying on research within the legal domain, potentially utilizing mapping between different legislation.

Broadening the scope technically, how could the proposed solution be adopted outside browsers? Can it be adapted to mobile apps or similar? These are both questions that would be interesting to explore in close relation to the domain of this thesis.

Other potential ideas include:

- Evaluating how cookies could be enhanced in order to support legal requirements, possibly without the need for browser-based mechanisms
- Explore the concept of provable consent, where cryptographic proof or similar can be used by the data controller to prove a valid consent
- What is the effect of ad blockers on legal compliance? How should data controllers adapt, or should they not?

Hopefully some, if not all, of the above-mentioned ideas will spark joy or excitement, motivating to further explore this important topic of the future.



Bibliography

[1] Carlisle Adams, Yu Dai, Catherine DesOrmeaux, Sean McAvoy, NamChi Nguyen, and Francisco Trindade. "Strengthening Enforcement in a Comprehensive Architecture for Privacy Enforcement at Internet Websites." In: *Frontiers in Computer Science* 2 (2020), p. 2. ISSN: 2624-9898. DOI: 10.3389/fcomp.2020.00002.

[2] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. "An XPath-Based Preference Language for P3P." In: *Proceedings of the 12th International Conference on World Wide Web*. WWW '03. Budapest, Hungary: Association for Computing Machinery, 2003, pp. 629–639. DOI: 10.1145/775152.775241.

[3] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. "XPref: a preference language for P3P." In: *Computer Networks* 48.5 (2005). Web Security, pp. 809–827. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2005.01.004.

[4] Abdulrahman Alabduljabbar, Ahmed Abusnaina, Ülkü Meteriz-Yildiran, and David Mohaisen. "TLDR: Deep Learning-Based Automated Privacy Policy Annotation with Key Policy Highlights." In: *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. WPES'21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 103–118. DOI: 10.1145/3463676.3485608.

[5] Apple. *Tracking Prevention in WebKit*. Dec. 1, 2020. URL: https://webkit.org/tracking-prevention/ (visited on 05/26/2022).

[6] Hany F. Atlam, Madini O. Alassafi, Ahmed Alenezi, Robert John Walters, and Gary B. Wills. "XACML for Building Access Control Policies in Internet of Things." In: *Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security, IoTBDS 2018, Funchal, Madeira, Portugal, March 19-21, 2018*. Ed. by Víctor Méndez Muñoz, Gary B. Wills, Robert John Walters, Farshad Firouzi, and Victor Chang. SciTePress, 2018, pp. 253–260. DOI: 10.5220/0006725102530260.

[7] Adam Barth. *HTTP State Management Mechanism*. Internet Requests for Comments. Apr. 2011. DOI: 10.17487/RFC6265.

[8] Stefan Becher, Armin Gerl, and Bianca Meier. "Don't Forget the User: From User Preferences to Personal Privacy Policies." In: *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)*. Deggendorf, Germany: IEEE, Sept. 2020, pp. 774–778. DOI: 10.1109/ACIT49673.2020.9208810.

[9] Mo Becker, Alexander Malkis, and Laurent Bussard. *A Framework for Privacy Preferences and Data-Handling Policies*. Tech. rep. MSR-TR-2009-128. Sept. 2009. URL: https://www.microsoft.com/en-us/research/publication/a-framework-for-privacy-preferences-and-data-handling-policies/.

[10] Mike Belshe, Roberto Peon, and Martin Thomson. *Hypertext Transfer Protocol Version 2 (HTTP/2)*. Tech. rep. 7540. May 2015. 96 pp. DOI: 10.17487/RFC7540.

[11] Robin Berjon, Sebastian Zimmeck, Ashkan Soltani, David Harbage, and Peter Snyder. *Global Privacy Control (GPC)*. Proposal. Jan. 2022. URL: https://globalprivacycontrol.github.io/gpc-spec/.

[12] Mike Bishop. *Hypertext Transfer Protocol Version 3 (HTTP/3)*. Internet-Draft draft-ietf-quic-http-34. Work in Progress. Internet Engineering Task Force, Feb. 2021. 75 pp. URL: https://datatracker.ietf.org/doc/html/draft-ietf-quic-http-34.

[13] Duc Bui, Kang G. Shin, Jong-Min Choi, and Junbum Shin. "Automated Extraction and Presentation of Data Practices in Privacy Policies." In: *Proceedings on Privacy Enhancing Technologies* 2021.2 (Apr. 2021), pp. 88–110. DOI: 10.2478/popets-2021-0019.

[14] Denis Butin and Daniel Le Métayer. "A Guide to End-to-End Privacy Accountability." In: *2015 IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity*. Florence, Italy: IEEE, May 2015, pp. 20–25. DOI: 10.1109/TELERISE.2015.12.

[15] State of California Department of Justice Attorney General. *California Consumer Privacy Act (CCPA)*. URL: https://oag.ca.gov/privacy/ccpa (visited on 04/03/2022).

[16] State of California Department of Justice Attorney General. "California Consumer Privacy Act Regulations." In: *California Code of Regulations* Title 11. Division 1. Chapter 20 (2018). URL: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.

[17] Jason Castiglione, Dusko Pavlovic, and Peter-Michael Seidel. "Privacy Protocols." In: *Foundations of Security, Protocols, and Equational Reasoning: Essays Dedicated to Catherine A. Meadows*. Ed. by Joshua D. Guttman, Carl E. Landwehr, José Meseguer, and Dusko Pavlovic. Cham: Springer International Publishing, 2019, pp. 167–191. DOI: 10.1007/978-3-030-19052-1_12.

[18] Lily Chen, Steven Englehardt, Mike West, and John Wilander. *Cookies: HTTP State Management Mechanism*. Internet-Draft draft-ietf-httpbis-rfc6265bis-10. Work in Progress. Internet Engineering Task Force, Apr. 2022. 60 pp. URL: https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-rfc6265bis-10.

[19] Rex Chen, Fei Fang, Thomas Norton, Aleecia M. McDonald, and Norman Sadeh. "Fighting the Fog: Evaluating the Clarity of Privacy Disclosures in the Age of CCPA." In: *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. WPES'21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 73–102. DOI: 10.1145/3463676.3485601.

[20] European Commission. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018*. Brussels, Jan. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0043.

[21] Lorrie Cranor, Marc Langheinrich, and Massimo Marchiori. *A P3P Preference Exchange Language 1.0 (APPEL1.0)*. W3C Working Draft. W3C, Apr. 2004. URL: https://www.w3.org/TR/2002/WD-P3P-preferences-20020415/.

[22] Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, and Joseph Reagle. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. W3C Obsolete Recommendation. W3C, Aug. 2018. URL: https://www.w3.org/TR/2018/OBSL-P3P-20180830/.

[23] Lorrie Faith Cranor. "P3P: Making Privacy Policies More Useful." In: *IEEE Security Privacy* 1.6 (Nov. 2003), pp. 50–55. ISSN: 1558-4046. DOI: 10.1109/MSECP.2003.1253568.

[24] Frederic Debusseré. "The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?" In: *International Journal of Law and Information Technology* 13.1 (2005), pp. 70–97. ISSN: 0967-0769. DOI: 10.1093/ijlit/eai003.

[25] Henry DeYoung, Deepak Garg, Limin Jia, Dilsun Kaynar, and Anupam Datta. "Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws." In: *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society*. WPES'10. Chicago, Illinois, USA: Association for Computing Machinery, 2010, pp. 73–82. DOI: 10.1145/1866919.1866930.

[26] NOYB – European Center for Digital Rights. *noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints*. May 31, 2021. URL: https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints (visited on 05/23/2022).

[27] Nick Doty, Heather West, Justin Brookman, Sean Harvey, and Erica Newland. *Tracking Compliance and Scope*. W3C Working Group Note. W3C, Jan. 2019. URL: https://www.w3.org/TR/2019/NOTE-tracking-compliance-20190122/.

[28] Interactive Advertising Bureau Europe. *TCF – Transparency & Consent Framework*. URL: https://iabeurope.eu/transparency-consent-framework/ (visited on 01/17/2022).

[29] Adrienne Porter Felt, Serge Egelman, Matthew Finifter, Devdatta Akhawe, and David Wagner. "How to Ask for Permission." In: *7th USENIX Workshop on Hot Topics in Security (HotSec 12)*. Bellevue, WA: USENIX Association, Aug. 2012. URL: https://www.usenix.org/conference/hotsec12/workshop-program/presentation/Felt.

[30] Roy Fielding. *Apache does not tolerate deliberate abuse of open standards*. https://github.com/apache/httpd. Aug. 2012.

[31] Roy T. Fielding, Henrik Nielsen, Jeffrey Mogul, Jim Gettys, and Tim Berners-Lee. *Hypertext Transfer Protocol – HTTP/1.1*. Tech. rep. 2068. Jan. 1997. 162 pp. DOI: 10.17487/RFC2068.

[32] Roy T. Fielding and Julian Reschke. *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. Internet Requests for Comments. June 2014. DOI: 10.17487/RFC7230.

[33] Roy T. Fielding and Julian Reschke. *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*. Internet Requests for Comments. 2014. DOI: 10.17487/RFC7231.

[34] Roy T. Fielding and David Singer. *Tracking Preference Expression (DNT)*. W3C Working Group Note. W3C, Jan. 2019. URL: https://www.w3.org/TR/2019/NOTE-tracking-dnt-20190117/.

[35] Glenn Fleishman. "How the tragic death of Do Not Track ruined the web for everyone." In: *Fast Company* (Mar. 17, 2019). URL: https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone (visited on 01/04/2022).

[36] Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova, and Stefano Calzavara. "On Compliance of Cookie Purposes with the Purpose Specification Principle." In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 2020, pp. 326–333. DOI: 10.1109/EuroSPW51379.2020.00051.

[37] The Electronic Frontier Foundation. *A privacy-friendly Do Not Track (DNT) Policy*. May 25, 2018. URL: https://www.eff.org/dnt-policy (visited on 04/04/2022).

[38] Armin Gerl, Nadia Bennani, Harald Kosch, and Lionel Brunie. "LPL, Towards a GDPR-Compliant Privacy Language: Formal Definition and Usage." In: *Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVII*. Ed. by Abdelkader Hameurlain and Roland Wagner. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, pp. 41–80. DOI: 10.1007/978-3-662-57932-9_2.

[39] Colin M Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective." In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2021. DOI: 10.1145/3411764.3445779.

[40] Wentao Guo, Jay Rodolitz, and Eleanor Birrell. "Poli-See: An Interactive Tool for Visualizing Privacy Policies." In: *Proceedings of the 19th Workshop on Privacy in the Electronic Society*. WPES'20. Virtual Event, USA: Association for Computing Machinery, Nov. 2020, pp. 57–71. DOI: 10.1145/3411497.3420221.

[41] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. ""Okay, Whatever": An Evaluation of Cookie Consent Interfaces." In: *CHI Conference on Human Factors in Computing Systems*. CHI '22. New Orleans, LA, USA: Association for Computing Machinery, 2022. DOI: 10.1145/3491102.3501985.

[42] Catherine Han, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Narseo Vallina-Rodriguez, Amit Elazari, Kenneth A. Bamberger, and Serge Egelman. "The Price is (Not) Right: Comparing Privacy in Free and Paid Apps." In: *Proceedings on Privacy Enhancing Technologies* 2020.3 (2020), pp. 222–242. DOI: 10.2478/popets-2020-0050.

[43] Maximilian Hils, Daniel W. Woods, and Rainer Böhme. "Privacy Preference Signals: Past, Present and Future." In: *Proceedings on Privacy Enhancing Technologies* 2021.4 (2021), pp. 249–269. DOI: 10.2478/popets-2021-0069.

[44] Soheil Human and Florian Cech. "A Human-Centric Perspective on Digital Consenting: The Case of GAFAM." In: *Human Centred Intelligent Systems*. Ed. by Alfred Zimmermann, Robert J. Howlett, and Lakhmi C. Jain. Singapore: Springer Singapore, 2021, pp. 139–159. DOI: 10.1007/978-981-15-5784-2_12.

[45] Soheil Human, Max Schrems, Alan Toner, Gerben, and Ben Wagner. *Advanced Data Protection Control (ADPC)*. Unofficial Draft. Vienna, June 2021. URL: https://epub.wu.ac.at/8280/.

[46] Infrastrukturdepartementet. "Lag (2003:389) om elektronisk kommunikation [Swedish Electronic Communications Act]." In: *Svensk författningssamling* SFS 2003:389 (June 12, 2003). URL: http://rkrattsbaser.gov.se/sfst?bet=2003:389.

[47] Justitiedepartementet. "Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning [Act containing supplementary provisions to the EU General Data Protection Regulation]." In: *Svensk författningssamling* SFS 2018:218 (Apr. 19, 2018). URL: http://rkrattsbaser.gov.se/sfst?bet=2018:218.

[48] Saffija Kasem-Madani and Michael Meier. *Security and Privacy Policy Languages: A Survey, Categorization and Gap Identification*. 2015. arXiv: 1512.00201 [cs.CR].

[49] Rishabh Khandelwal, Thomas Linden, Hamza Harkous, and Kassem Fawaz. "PriSEC: A Privacy Settings Enforcement Controller." In: *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 465–482. ISBN: 978-1-939133-24-3. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/khandelwal.

[50] Soheil Khodayari and Giancarlo Pellegrino. "The State of the SameSite: Studying the Usage, Effectiveness, and Adequacy of SameSite Cookies." In: *2022 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, May 2022, pp. 312–329. DOI: 10.1109/SP46214.2022.00019.

[51] Sabrina Kirrane, Javier D Fernández, Wouter Dullaert, Uros Milosevic, Axel Polleres, Piero A Bonatti, Rigo Wenning, Olha Drozd, and Philip Raschke. "A Scalable Consent, Transparency and Compliance Architecture." In: *The Semantic Web: ESWC 2018 Satellite Events*. Ed. by Aldo Gangemi, Anna Lisa Gentile, Andrea Giovanni Nuzzolese, Sebastian Rudolph, Maria Maleshkova, Heiko Paulheim, Jeff Z Pan, and Mehwish Alam. Cham: Springer International Publishing, 2018, pp. 131–136. DOI: 10.1007/978-3-319-98192-5_25.

[52] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. "Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect." In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Aug. 2020, pp. 437–456. ISBN: 978-1-939133-16-8. URL: https://www.usenix.org/conference/soups2020/presentation/kitkowska.

[53] Graham Klyne, Mark Nottingham, and Jeffrey Mogul. *Registration Procedures for Message Header Fields*. Internet Requests for Comments. Sept. 2004. DOI: 10.17487/RFC3864.

[54] Konrad Kollnig, Ruben Binns, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb, and Nigel Shadbolt. "A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps." In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Aug. 2021, pp. 181–196. ISBN: 978-1-939133-25-0. URL: https://www.usenix.org/conference/soups2021/presentation/kollnig.

[55] Michael Kretschmer, Jan Pennekamp, and Klaus Wehrle. "Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web." In: *ACM Trans. Web* 15.4 (July 2021). ISSN: 1559-1131. DOI: 10.1145/3466722.

[56] Chiara Krisam, Heike Dietmann, Melanie Volkamer, and Oksana Kulyk. "Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites." In: *European Symposium on Usable Security 2021*. EuroUSEC '21. Karlsruhe, Germany: Association for Computing Machinery, 2021, pp. 1–8. DOI: 10.1145/3481357.3481516.

[57] IAB Tech Lab. *Ads.txt – Authorized Digital Sellers*. URL: https://iabtechlab.com/ads-txt/ (visited on 03/18/2022).

[58] Daniel Le Métayer. "A Formal Privacy Management Framework." In: *Formal Aspects in Security and Trust*. Ed. by Pierpaolo Degano, Joshua Guttman, and Fabio Martinelli. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 162–176. DOI: 10.1007/978-3-642-01465-9_11.

[59] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. "The Privacy Policy Landscape After the GDPR." In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (Jan. 2020), pp. 47–64. DOI: 10.2478/popets-2020-0004.

[60] Dominique Machuletz and Rainer Böhme. "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR." In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (2020), pp. 481–498. DOI: 10.2478/popets-2020-0037.

[61] Célestin Matte, Nataliia Bielova, and Cristiana Santos. "Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework." In: *2020 IEEE Symposium on Security and Privacy (SP)*. May 2020, pp. 791–809. DOI: 10.1109/SP40000.2020.00076.

[62] Célestin Matte, Cristiana Santos, and Nataliia Bielova. "Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?" In: *Privacy Technologies and Policy*. Ed. by Luís Antunes, Maurizio Naldi, Giuseppe F Italiano, Kai Rannenberg, and Prokopios Drogkaris. Cham: Springer International Publishing, 2020, pp. 163–185. DOI: 10.1007/978-3-030-55196-4_10.

[63] Michael J. May, Carl A. Gunter, and Insup Lee. "Privacy APIs: access control techniques to analyze and verify legal privacy policies." In: *19th IEEE Computer Security Foundations Workshop (CSFW'06)*. Venice, Italy: IEEE, July 2006, 13 pp.–97. DOI: 10.1109/CSFW.2006.24.

[64] Maryam Mehrnezhad, Kovila Coopamootoo, and Ehsan Toreini. "How Can and Would People Protect From Online Tracking?" In: *Proceedings on Privacy Enhancing Technologies* 2022.1 (2022), pp. 105–125. DOI: 10.2478/popets-2022-0006.

[65] Microsoft. *P3P is no longer supported*. Dec. 15, 2016. URL: https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/mt146424(v=vs.85) (visited on 03/15/2022).

[66] Lou Montulli and David M. Kristol. *HTTP State Management Mechanism*. Tech. rep. 2109. Feb. 1997. 21 pp. DOI: 10.17487/RFC2109.

[67] Lou Montulli and David M. Kristol. *HTTP State Management Mechanism*. Internet Requests for Comments. Oct. 2000. DOI: 10.17487/RFC2965.

[68] Victor Morel and Raúl Pardo. "SoK: Three Facets of Privacy Policies." In: *Proceedings of the 19th Workshop on Privacy in the Electronic Society*. WPES'20. Virtual Event, USA: Association for Computing Machinery, 2020, pp. 41–56. DOI: 10.1145/3411497.3420216.

[69] Mozilla. *Enhanced Tracking Protection in Firefox for desktop*. URL: https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop (visited on 05/26/2022).

[70] Daniela Napoli, Khadija Baig, Sana Maqsood, and Sonia Chiasson. ""I'm Literally Just Hoping This Will Work:'' Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities." In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Aug. 2021, pp. 263–280. ISBN: 978-1-939133-25-0. URL: https://www.usenix.org/conference/soups2021/presentation/napoli.

[71] Henrik Nielsen, Roy T. Fielding, and Tim Berners-Lee. *Hypertext Transfer Protocol – HTTP/1.0*. RFC 1945. RFC Editor, May 1996. DOI: 10.17487/RFC1945.

[72] Henrik Nielsen, Jeffrey Mogul, Larry M Masinter, Roy T. Fielding, Jim Gettys, Paul J. Leach, and Tim Berners-Lee. *Hypertext Transfer Protocol – HTTP/1.1*. Tech. rep. 2616. June 1999. 176 pp. DOI: 10.17487/RFC2616.

[73] Mark Nottingham. *Well-Known Uniform Resource Identifiers (URIs)*. Internet Requests for Comments. May 2019. DOI: 10.17487/RFC8615.

[74] Mark Nottingham and Jeffrey Mogul. *HTTP Header Field Registrations*. Internet Requests for Comments. Dec. 2005. DOI: 10.17487/RFC4229.

[75] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence." In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI '20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–13. DOI: 10.1145/3313831.3376321.

[76] Sean O'Connor, Ryan Nurwono, Aden Siebel, and Eleanor Birrell. "(Un)Clear and (In)Conspicuous: The Right to Opt-out of Sale under CCPA." In: *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. WPES'21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 59–72. DOI: 10.1145/3463676.3485598.

[77] Information Commissioner's Office. *ICO to call on G7 countries to tackle cookie pop-ups challenge*. Sept. 7, 2021. URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/09/ico-to-call-on-g7-countries-to-tackle-cookie-pop-ups-challenge/ (visited on 05/23/2022).

[78] Emmanouil Papadogiannakis, Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos P. Markatos. "User Tracking in the Post-Cookie Era: How Websites Bypass GDPR Consent to Track Users." In: *Proceedings of the Web Conference 2021*. WWW'21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 2130–2141. DOI: 10.1145/3442381.3450056.

[79] Stuart L Pardau. "The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States." In: *Journal of Technology Law & Policy* 23.1 (2018), pp. 68–114.

[80] The European Parliament and the Council of the European Union. "Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services." In: *Official Journal of the European Union* L 241 (Sept. 17, 2015), pp. 1–15. URL: http://data.europa.eu/eli/dir/2015/1535/oj.

[81] The European Parliament and the Council of the European Union. "Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)." In: *Official Journal of the European Union* L 321 (Dec. 17, 2018), pp. 36–214. URL: http://data.europa.eu/eli/dir/2018/1972/oj.

[82] 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)." In: *Official Journal of the European Union* L 201 (July 31, 2002), pp. 37–47. URL: http://data.europa.eu/eli/dir/2002/58/oj.

[83] The European Parliament and the Council of the European Union. "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." In: *Official Journal of the European Union* L 337 (Dec. 18, 2009), pp. 11–36. URL: http://data.europa.eu/eli/dir/2009/136/oj.

[84] The European Parliament and the Council of the European Union. "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." In: *Official Journal of the European Union* L 281 (Nov. 23, 1995), pp. 31–50. URL: http://data.europa.eu/eli/dir/1995/46/oj.

[85] The European Parliament and the Council of the European Union. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." In: *Official Journal of the European Union* L 119 (May 4, 2016), pp. 1–88. URL: http://data.europa.eu/eli/reg/2016/679/oj.

[86] Article 29 Data Protection Working Party. *Opinion 2/2010 on online behavioural advertising*. Opinion 00909/10/EN WP 171. European Commission, June 22, 2010. 24 pp. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf.

[87] Article 29 Data Protection Working Party. *Working Document 02/2013 providing guidance on obtaining consent for cookies*. Working Document 1676/13/EN WP 208. European Commission, Oct. 2, 2013. 6 pp. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.

[88] Lucian Popa, Ali Ghodsi, and Ion Stoica. "HTTP as the Narrow Waist of the Future Internet." In: *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. Hotnets-IX. Monterey, California: Association for Computing Machinery, Oct. 2010, pp. 1–6. DOI: 10.1145/1868447.1868453.

[89] Yves Poullet. "Is the general data protection regulation the solution?" In: *Computer Law & Security Review* 34.4 (2018), pp. 773–778. ISSN: 0267-3649. DOI: https://doi.org/10.1016/j.clsr.2018.05.021.

[90] Gaston Pugliese, Christian Riess, Freya Gassmann, and Zinaida Benenson. "Long-Term Observation on Browser Fingerprinting: Users' Trackability and Perspective." In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (2020), pp. 558–577. DOI: 10.2478/popets-2020-0041.

[91] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. "Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control." In: *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. Asia CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 340–351. DOI: 10.1145/3321705.3329806.

[92] Cristiana Santos, Nataliia Bielova, and Célestin Matte. "Are cookie banners indeed compliant with the law?" In: *Technology and Regulation* 2020 (2020), pp. 91–135. DOI: 10.26116/techreg.2020.009.

[93] Cristiana Santos, Midas Nouwens, Michael Toth, Nataliia Bielova, and Vincent Roca. "Consent Management Platforms Under the GDPR: Processors and/or Controllers?" In: *Privacy Technologies and Policy*. Ed. by Nils Gruschka, Luís Filipe Coelho Antunes, Kai Rannenberg, and Prokopios Drogkaris. Cham: Springer International Publishing, 2021, pp. 47–69. DOI: 10.1007/978-3-030-76663-4_3.

[94] Cristiana Santos, Arianna Rossi, Lorena Sanchez Chamorro, Kerstin Bongard-Blanchy, and Ruba Abu-Salma. "Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens." In: *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. WPES'21. Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, pp. 187–194. DOI: 10.1145/3463676.3485611.

[95] Theodor Schnitzler, Shujaat Mirza, Markus Dürmuth, and Christina Pöpper. "SoK: Managing Longitudinal Privacy of Publicly Shared Personal Online Data." In: *Proceedings on Privacy Enhancing Technologies* 2021.1 (Jan. 2021), pp. 229–249. DOI: 10.2478/popets-2021-0013.

[96] Jean-Pierre Smith, Prateek Mittal, and Adrian Perrig. "Website Fingerprinting in the Age of QUIC." In: *Proceedings on Privacy Enhancing Technologies* 2021.2 (2021), pp. 48–69. DOI: 10.2478/popets-2021-0017.

[97] Daniel Smullen, Yaxing Yao, Yuanyuan Feng, Norman Sadeh, Arthur Edelstein, and Rebecca Weiss. "Managing Potentially Intrusive Practices in the Browser: A User-Centered Perspective." In: *Proceedings on Privacy Enhancing Technologies* 2021.4 (2021), pp. 500–527. DOI: 10.2478/popets-2021-0082.

[98] California Secretary of State. "Proposition 24: The California Privacy Rights Act of 2020." In: *Text of Proposed Laws* California General Election Nov. 3, 2020 (2020), pp. 42–75. URL: https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.

[99] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "Awareness, Adoption, and Misconceptions of Web Privacy Tools." In: *Proceedings on Privacy Enhancing Technologies* 2021.3 (2021), pp. 308–333. DOI: 10.2478/popets-2021-0049.

[100] Theeraporn Suphakul and Twittie Senivongse. "Development of Privacy Design Patterns Based on Privacy Principles and UML." In: *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. Kanazawa, Japan: IEEE, June 2017, pp. 369–375. DOI: 10.1109/SNPD.2017.8022748.

[101] Erik Sy, Tobias Mueller, Christian Burkert, Hannes Federrath, and Mathias Fischer. "Enhanced Performance and Privacy for TLS over TCP Fast Open." In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (Apr. 2020), pp. 271–287. DOI: 10.2478/popets-2020-0027.

[102] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. "Deciding on Personalized Ads: Nudging Developers About User Privacy." In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Aug. 2021, pp. 573–596. ISBN: 978-1-939133-25-0. URL: https://www.usenix.org/conference/soups2021/presentation/tahaei.

[103] Jenny Tang, Hannah Shoemaker, Ada Lerner, and Eleanor Birrell. "Defining Privacy: How Users Interpret Technical Terms in Privacy Policies." In: *Proceedings on Privacy Enhancing Technologies* 2021.3 (July 2021), pp. 70–94. DOI: 10.2478/popets-2021-0038.

[104] Giorgio Di Tizio and Fabio Massacci. "A Calculus of Tracking: Theory and Practice." In: *Proceedings on Privacy Enhancing Technologies* 2021.2 (2021), pp. 259–281. DOI: 10.2478/popets-2021-0027.

[105] Martino Trevisan, Stefano Traverso, Eleonora Bassi, and Marco Mellia. "4 Years of EU Cookie Law: Results and Lessons Learned." In: *Proceedings on Privacy Enhancing Technologies* 2019.2 (2019), pp. 126–145. DOI: 10.2478/popets-2019-0023. URL: https://doi.org/10.2478/popets-2019-0023.

[106] Max-R. Ulbricht and Frank Pallas. "YaPPL - A Lightweight Privacy Preference Language for Legally Sufficient and Automated Consent Provision in IoT Scenarios." In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Ed. by Joaquin Garcia-Alfaro, Jordi Herrera-Joancomartí, Giovanni Livraga, and Ruben Rios. Cham: Springer International Publishing, 2018, pp. 329–344. DOI: 10.1007/978-3-030-00305-0_23.

[107] United Nations General Assembly. *Universal Declaration of Human Rights*. United Nations, Dec. 1948. URL: https://www.un.org/sites/un2.un.org/files/udhr.pdf.

[108] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. "(Un)Informed Consent: Studying GDPR Consent Notices in the Field." In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS '19. London, United Kingdom: Association for Computing Machinery, 2019, pp. 973–990. DOI: 10.1145/3319535.3354212.

[109] Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Chris Hanson, James Hendler, Lalana Kagal, and Gerald Jay Sussman. "Transparency and End-to-End Accountability: Requirements for Web Privacy Policy Languages." In: *Proceedings of W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*. Ispra, Italy, Oct. 2006. URL: https://www.w3.org/2006/07/privacy-ws/papers/34-weitzner-transparency-accountability/.

[110] Daniel J. Weitzner, Jim Hendler, Tim Berners-Lee, and Dan Connolly. "Creating the Policy-Aware Web: Discretionary, Rules-based Access for the World Wide Web." In: *Web and Information Security*. Ed. by Elena Ferrari and Bhavani Thuraisingham. Hershey, PA: IGI Global, Jan. 2006, pp. 1–31. DOI: 10.4018/978-1-59140-588-7.ch001.

[111] Zhiju Yang and Chuan Yue. "A Comparative Measurement Study of Web Tracking on Mobile and Desktop Environments." In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (2020), pp. 24–44. DOI: 10.2478/popets-2020-0016.

[112] Jun Zhao, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. "Privacy Languages: Are We There yet to Enable User Controls?" In: *Proceedings of the 25th International Conference Companion on World Wide Web*. WWW '16 Companion. Montréal, Québec, Canada: International World Wide Web Conferences Steering Committee, 2016, pp. 799–806. DOI: 10.1145/2872518.2890590.

[113] Sebastian Zimmeck and Kuba Alicki. "Standardizing and Implementing Do Not Sell." In: *Proceedings of the 19th Workshop on Privacy in the Electronic Society*. WPES'20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 15–20. DOI: 10.1145/3411497.3420224.

A Appendix

A.1 Additional feature ideas

As a side effect of compiling the presented features, numerous ideas for additional features arose but where outside the immediate scope of properties defined and as such were not motivated as part of this thesis' suggestions. This section will list them to make them available, but the ideas are not to be considered as part of the result.

- Consent settings cookie
  - Provide the user's consent configuration of a website as a `__consent` cookie, allowing to communicate preferences in queries to servers for data controllers to respect.
  - The consent cookie should be read-only from a server perspective, and only editable through the browser interface.
  - Implement support for allowing this cookie to be persistent between sessions and between sandboxed environments such as tab sandboxes and private/incognito mode.
- Enforce documentation of cookies
  - Browsers should either block cookies or warn the user if the server is requesting to use undocumented cookies/trackers. The server/data controller should be informed of in what way(s) non-compliance was found and action taken by the browser. For relaxation, different levels could be utilized:
    * STRICT: Block all undocumented cookies
    * LAX: Allow `necessary` undocumented cookies but warn the user; block the remaining undocumented cookies
    * NONE: Allow all undocumented cookies, but warn the user
  - Cookies that do not have corresponding documentation should be blocked by default. Necessary cookies could be allowed by default but alerting the user and allowing for the user to block such cookies by changing the STRICT/LAX/NONE setting (that can be possible on a per-website basis).

- Communicate strict enforcement of ADPC+, requiring the server/data controller to comply to utilize cookies. Inspired by HTTP Strict Transport Security, a `Strict-ADPC` header or similar can be added to requests to inform and require the server to comply.
- Expand the `necessary` attribute to allow consent for a balanced period (e.g., a week, month, or similar) for certain appliances such as website settings.
- Enable disallowing of third-party cookies as part of ADPC+ settings and communicate the preference through HTTP headers such as `Cookies: disallow-3rd-party` or similar.
- Implement a privacy notification icon to inform users of ADPC+ compliance, similar to the padlock icon used for notifying a secure/encrypted connection.
- Implement the use for rudimentary ADPC+ exchange in the TCP handshake through TCP Fast Open, to enable some speed gains from informing the server early on regarding vital ADPC+ requirements.