Bridging the Privacy Gap: Enhanced User Consent Mechanisms on the Web

Carl Magnus Bruhner*, David Hasselquist*†, Niklas Carlsson*
*Linköping University, Sweden
†Sectra Communications, Sweden

***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 web users. Privacy banners in all shapes and sizes ask for permission through more or less challenging designs and make privacy control more of a struggle than they help users' privacy. In this paper, we present a novel solution expanding the *Advanced Data Protection Control* (ADPC) mechanism to bridge current gaps in user data and privacy control. Our solution moves the consent control to the browser interface to give users a seamless and hassle-free experience, while at the same time offering content providers a way to be legally compliant with legislation. Through an extensive review, we evaluate previous works and identify current gaps in user data control. We then present a blueprint for future implementation and suggest features to support privacy control online for users globally. Given browser support, the solution provides a tangible path to effectively achieve legally compliant privacy and consent control in a user-oriented manner that could allow them to again browse the web seamlessly.**

I. Introduction

Have you ever found yourself bombarded with cookie and privacy banners asking for your consent? 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"* [41].

The current state of privacy control is everything but satisfactory. Research shows that most cookie banners do not comply with legal requirements [69], [55], [28], [71], incorrect consent signals spread via connected consent management providers [55], and the user experience is heavily burdened by interruptions with consent dialogs for every newly visited website [33]. Using private browsing only worsen some of these problems; e.g., by increasing the interruptions to every initial visit of every new session. Current practices are particularly troublesome for users with visual disabilities [62].

Privacy control is non-trivial as many aspects must be considered from several perspectives, including legal requirements, technical challenges, and the user experience. Furthermore, unlike secrecy and authenticity, privacy is not a security requirement but a fundamental social right [15]. Not being subject of arbitrary interference of one's privacy is the 12^{th} article of the UN Declaration of Human Rights [89]. This makes privacy both a technical and legislative challenge. To ensure privacy, numerous legislations have been introduced, including *General Data Protection Regulation* (GDPR) in 2018 and *California Consumer Privacy Act* (CCPA) in 2020.

Safeguarding user consent plays a central role in such user privacy legislation. However, many solutions satisfying such legal requirements do not always result in the best user experiences and often come with their own technical challenges. It is clear that the technical and legislative development affect each other, with technical solutions adapting to legislation and, vice versa, gaining support from legislation as well [76], [37].

Privacy policies on the web provide one example of a battle between technical support and legislation, where privacy policies tend to be too complex with widespread misconceptions [81]. With modern privacy legislation, more pressure has been put on data and service providers to ensure valid consent for collecting user information [69], [65]. While website and online advertisement providers increasingly comply with such new laws and regulations, little has changed from a browser and protocol perspective. For example, despite several proposed solutions [37], [60], especially using machine learning [5], [13], [43], none of these solutions have made their way into every-day use.

In fact, even though GDPR and European legislators explicitly mention browser settings as a way to express consent [85], [8] and even though it can be considered as the best solution for managing cookie consent [71], there has not yet been any widespread or compliant support [69]. A browser implementation could from a user perspective save time, make it easier, and enforce privacy rights. For a website provider and data controller perspective, it could ensure legal compliance and ensure that the information and consent is correctly presented and expressed. We believe that the global dissatisfaction with the current state and current legislation efforts make this an ideal time to implement and deploy a new browser-based solution. However, as seen by the current status, it is important that such a solution satisfies the right criteria.

In this paper, we present a browser-based consent management solution motivated by the privacy gaps and ten important privacy mechanism properties (that we identified via a literature review) needed to achieve legally compliant privacy and consent control. The solution expands on the *Advanced Data Protection Control* (ADPC), considers current legal and technical requirements, and better put the user in control than previous proposals. Our solution is novel and aims to ensure compliance with privacy regulations such as GDPR

Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2023
3 March 2023, San Diego, CA, USA
ISBN 1-891562-87-8
https://dx.doi.org/10.14722/madweb.2023.23017
www.ndss-symposium.org

and CCPA.[1] Our contributions are broken into three parts.

First, we review the current state of web privacy and identify the gaps in user privacy control (Section II). Here, we identify current challenges and solutions to find the prevalent gaps that need to be addressed. Then, from legal requirements and previous research, we present ten consent mechanism properties that are important to achieve legally compliant privacy and consent control.

Second, we review existing browser-based consent mechanisms, compare them with regards to the ten identified properties, formulate requirements, and suggest improvements that need to be addressed to better satisfy these properties (Section III). Here, we bridge the gaps by presenting a gap analysis of current and previous browser-based consent mechanisms.

Third, we combine the suggested improvements into an improved version of ADPC that we call ADPC+ and describe how ADPC+ can be both implemented and put to use (Section IV). To put it all together, we present five features that together with legislation satisfy all the ten desirable properties. To ease implementation and maximize the chance for practical use, the five features are designed as improvements to the existing browser-based mechanism ADPC. We also evaluate the features with regards to how well they satisfy the proposed properties (individually and in combination), discuss implementation incentives, and provide an implementation roadmap including feature dependencies and division of responsibilities.

The paper is concluded with a discussion of related works (Section V) and our conclusions (Section VI).

II. Identifying the gaps

Through a review of current best practices and the literature, we have identified clear privacy gaps in the current user consent mechanisms and ten properties that need to be fulfilled for legally compliant privacy and consent control. This section first describes some common patterns identified, recurring recommendations, and legal requirements brought forward in prior research. Based on the review, we then outline the ten desirable properties we expect that an ideal solution should satisfy. In later sections we use these properties to compare different solutions to an "ideal" solution that satisfies all ten properties. Of course, these are not the only properties and considerations that a practical system must consider.

A. Current state of web privacy

Cookie usage and opting in/out: Sanchez-Rola et al. [68] show that more than 90% of the visited websites use cookies that could identify users and that opting out from tracking is both difficult and ineffective. Due to improperly implemented opt-out features, many users that would desire to opt-out are therefore today tracked with long-lasting cookies. Smullen et al. [74] study potentially intrusive practices, including privacy-related practices such as behavioral profiling, reporting and analytics, targeted ads, identity, sign-in services, and fingerprinting. Here, 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. Similarly, a recent study of privacy-enhancing technologies on the top-100 EU websites conclude that opting out of tracking, especially when previously opted in, is very difficult [58]. How to opt-out varies greatly, with the most common ways offered being to contact service providers and changing browser settings.

Cookie descriptions, consenting, and dark patterns: A widespread phenomenon is the use of "dark patterns"; i.e., designs that manipulatively steer users in a deceiving or predetermined direction such as accepting or selecting certain options in cookie banners [31], [64]. Large organizations like Google and Facebook have been found and criticized for utilizing such dark patterns, instead of empowering end users [38]. Examples of dark patterns include unequal paths, where the most and least privacy-protective choices have unequal interaction paths, and "confirm-shaming", where wordings use guilt or shame to influence a decision [33]. As a reaction, several legal initiatives have been introduced to prohibit various dark patterns, including GDPR requiring withdrawal of consent to be as easy as giving consent [64], [69].

Previous works have studied the prevalence of dark patterns. Krisam et al. [49] examine and classify cookie disclaimers of popular websites, finding that over 85% use dark patterns. Only a little bit over 20% of the websites offered a one-click option for rejecting all cookies; thus, not complying with the requirement of balanced choice. Machuletz and Böhme [54] show that users tend to accept cookies to a greater extent when the consent dialog uses dark patterns with a visibly default accept button.

Within the scope of dark patterns, Gray et al. [31] analyze three types of consent banners and conclude that there is much to be done to combine, e.g., design, law, and ethics, to prevent the use of dark patterns and empower users. Habib et al. [33] also study 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 confirm-shaming. Utz et al. [90] show that 72% of users interacting with a consent notice did so because they were annoyed, and only 10% interacted to protect their privacy.

Santos et al. [71] show that nearly 90% of cookie banners violate applicable laws, with most banners being vague in their purpose description. Other violations include deviations from freely given consent through the use of positive and negative framing, and absence of essential information necessary for an informed consent. An earlier study by Fouad et al. [28] supports this view, showing that 95% of cookies used on websites do not have an explicitly declared purpose.

Provider-based consent mechanisms: Besides browser-based consent technology, there have been some initiatives from the content providers as well, especially in the wake of the *ePrivacy Directive* (ePD) cookie amendment and cookie policies [20], [83], [84]. One category is consent management platforms that offer content providers functionalities like cookie banners and legal data processing conformity [48]. 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 [55]. One leading platform, considered to be a de facto standard [70], is the *Transparency and Consent Frame-*

[1] While closely related to the legal domain, this is not our focus. Instead, we rely on research within the technical–legal domain and current legislation.

work (TCF) [40], standardized by the European branch of the *Interactive Advertising Bureau* (IAB). TCF aims to provide GDPR compliance for the digital advertising industry, though compliance has been widely questioned [31], [37], [55], [69], [70]. The 20-year-old *Network Advertising Initiative* (NAI) is another initiative that has not been widely adopted [37].

GDPR and other privacy legislation violations can easily spread with multi-site cookies. On this topic, Matte et al. [55] show that positive consent is stored in shared cookies for several websites even though the user has explicitly opted out. It should also be noted that initiatives to limit multi-site cookies implicitly require developers to be aware of policy implications to avoid unknowingly introducing security and privacy vulnerabilities [44]. Another study by Matte et al. [56] show significant variations in how advertisers use consent or legitimate interest as a basis for data processing, even for purposes that arguably should rely on consent. Santos et al. [70] explore similar effects of less compliant CMPs and conclude that CMPs in many cases qualify as data controllers. Kyi et al. [50] empirically investigate the use of deceptive designs of legitimate interests. Nouwens et al. [64] look at dark patterns of CMP designs, finding that only 12% meet minimal requirements of European law, and confirm that dark patterns lead to increased consent.

Legislative compliance: Trevisan et al. [87] study the impact of the ePD prior to GDPR, showing 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, finding no significant difference in exposure to tracking technologies. Kretschmer et al. [48] study the impact of the GDPR on the web, concluding that even though GDPR has had an overall positive impact on privacy, there is still much room for improvement in terms of compliance. They find that most policies still lack required information or do not provide it in a user-friendly form, and that opting out is still often offered in inconvenient ways.

O'Connor et al. [65] take a CCPA perspective and study how websites offer opting out of selling one's data. As with GDPR cookie banners, using deceptive designs to trick users into accepting default settings is common, even though CCPA does not explicitly prohibit this. Chen et al. [16] study privacy policies of popular websites in the light of CCPA and survey consumers regarding how they interpret the policies. They show that both vagueness and ambiguity exist from several perspectives when interpreting CCPA and privacy policies.

B. Recommendations for improving web privacy

Aside from evaluating the current state of web privacy, many studies also provide recommendations and suggestions. We next summarize the most commonly recurring categories.

Standardization: Several studies [16], [28], [68], [70], [71], [87] suggest a more standardized structure to address issues such as vagueness and ambiguity [16], as well as to ease language tensions [71]. The standard should preferably be developed by a neutral party in contrast to content providers and similar parties [70]. Additionally, standardization can help with systematic and automatic auditing [28], [70], [87].

Necessity distinction: According to the ePD, the requirement of user consent to store information in the user's equipment does not include storage and access that are needed to enable communication or that are considered "strictly necessary" to provide the services the user explicitly requested [83, 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 [84, Rec. 66].

As noted by some, there is therefore a need for a clear distinction between necessary and unnecessary cookies [49], [71]. This can help determine if some cookies should be rejected by default [71] and clarify what is technically necessary from a legislative perspective [49]. A clear distinction also helps with standardized and automated auditing [28], [70], [87].

Browser solution: Technical standardization and the use of privacy-preserving technologies to minimize the use of personal data are suggested by several studies [48], [68], especially concerning using standardized settings in browsers [33], [49], [65], [71], [74]. Browser settings are motivated by properties like neutrality and usability [74], and legislation now supporting such technical solutions [33]. This is in contrast to previous initiatives that have been considered as either ahead of their time or too simplified [54].

C. Legal requirements on browser-based consent mechanisms

Santos et al. [69] provide an extensive review of legislative requirements and consent mechanisms on the web, presenting a list of 22 low-level requirements for valid consent through consent banner design. Table I show these requirements categorized into seven high-level requirements. To strengthen the foundation, we validate and map each requirement to previous works. Here, we denote the requirement as A1–A22.

Another categorization of legal requirements is presented in another study by Santos et al. [71], focusing on cookie banner text. Table II summarizes these requirements, denoted as B1–B6, and provide mappings to requirements A1–A22.

D. Desirable properties

A data controller is an entity that determines how and why personal data is processed (e.g., website owners or content providers) [85], while a data subject is an identified or identifiable natural person (e.g., users and website visitors) [85]. Ideally, a solution should serve both the data controller with ensuring legal compliance, and the data subject with privacy control. Based on the reviewed studies of current solutions, we identify a need for: (1) a more standardized and auditable approach to consent [16], [28], [68], [70], [71], [74], [87], (2) a clear distinction between necessary and unnecessary cookies [49], [71], and (3) technical enforcement of consent through browser mechanisms [33], [49], [65], [71], [74].

Combining the two sets of requirements (Tables I and II) with the identified needs, we end up with a set of desirable properties. Table III shows the ten proposed properties P1–P10, together with their rationale. Here, P1–P7 are based on consolidation of the legal requirements, and P8–P10 are based on the identified suggestions of current solutions.

III. Bridging the gaps

To bridge the identified privacy gaps and improve user consent control, this section first review previously proposed

TABLE I. LEGAL REQUIREMENTS ON CONSENT BANNER DESIGN AND IMPLEMENTATION WITH MAPPING TO SUPPORTING RESEARCH

Requirements [69]			**Previous example work**
High-level	**ID**	**Low-level**	
Prior	A1	Prior to storing an identifier	[55], [68], [69], [87]
	A2	Prior to sending an identifier	[68], [69], [87]
Free	A3	No merging into a contract	[69]
	A4	No tracking walls	[31], [69]
Specific	A5	Separate consent per purpose	[28], [55], [56], [69], [70], [71]
Informed	A6	Accessibility of information page	[65], [69]
	A7	Necessary information on browser-based tracking technology	[28], [69], [71]
	A8	Information on consent banner configuration	[69]
	A9	Information on the data controller	[69]
	A10	Information on rights	[69]
Unambiguous	A11	Affirmative action design	[33], [49], [55], [64], [68], [69]
	A12	Configurable banner	[31], [33], [49], [54], [55], [65], [68], [69]
	A13	Balanced choice	[31], [33], [49], [54], [55], [58], [64], [65], [69], [70]
	A14	Post-consent registration	[69]
	A15	Correct consent registration	[55], [69]
Readable and accessible	A16	Distinguishable	[65], [69]
	A17	Intelligible	[68], [69], [71]
	A18	Accessible	[31], [65], [69], [70]
	A19	Clear and plain language	[16], [28], [33], [69], [71]
	A20	No consent wall	[31], [48], [69]
Revocable	A21	Possible to change in the future	[33], [55], [58], [68], [69]
	A22	Delete "consent cookie" and communicate to third parties	[58], [68], [69]

TABLE II. LEGAL REQUIREMENTS ON COOKIE BANNER TEXT

Legal requirements [71]	**Mapping to A1–A22**
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, A4
B6: Informed consent	A7, A8, A9, A10

browser-based consent mechanisms and compare them with regards to the suggested properties (P1–P10). Then, we select the mechanism that fulfill most of the properties and suggest improvements that would help to better satisfy these properties.

A. Determining browser-based consent mechanism foundation

To strengthen the users' privacy, various standardizations and other initiatives have been proposed and implemented. We next present four browser-based examples.

Platform for Privacy Preferences Project (P3P): Originally published in 2002, P3P [18] was a promising initiative for user privacy supported by both Microsoft Internet Explorer and Netscape Navigator [19]. P3P standardized a way for websites to offer privacy policies so that, for instance, a browser can check whether the data collection that the website requests (through P3P) is acceptable according to the user's setting and thus can be allowed without need for user interaction. In the case that the request goes beyond what is allowed by default, P3P requires interactive user approval. There have been several initiatives based on P3P, including *A P3P Preferences Exchange Language* (APPEL) [17], designed to allow a user to express sets of preferences, and an XPath-based alternative [3]

TABLE III. 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, A2
P2	Freely given consent	Consent should be voluntary, not merged into a contract, and not forced with "tracking walls" blocking access without consent	A3, A4, 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–A10, B1.1, B6
P5	Unambiguous consent	An affirmative, balanced configurable choice with correct consent should be registered no earlier than after given consent	A11–A15
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–A20, B1.2, B1.3, B2–B4
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, A22
P8	Standardized	Purposes should be standardized and based on legal requirements to prevent uncertainty and additionally allowing for auditing	[16], [28], [68], [70], [71], [74], [87]
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–P8	[49], [71]
P10	Browser-controlled	Consent settings should be handled by the browser, with the browser signaling data subject's choice to the data controller	[33], [49], [65], [71], [74]

using the preference language XPref [4]. Microsoft supported P3P all the way to Microsoft Edge, but removed support in 2016 [59], before *World Wide Web Consortium* (W3C) obsoleted the project in 2018.

Do Not Track (DNT): DNT [26] was a W3C initiative for enabling user preferences, introducing the HTTP header field `DNT` where the browser could include the user's preference regarding tracking in requests sent to the server. The *Electronic Frontier Foundation* (EFF) expanded on the DNT initiative by creating a compliance policy utilizing the well-known URI structure for standardization [82]. This way a domain can communicate that it respects DNT.

The end of DNT started back in 2012 when Microsoft shipped Internet Explorer 10 with DNT activated by default [27]. 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 [24]). The Tracking Protection Working Group of W3C finally concluded its work in 2019, thus putting an official end to DNT [22].

Global Privacy Control (GPC): GPC [12] 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 [75]. 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 [76]. The timing of GPC in the new legislative

landscape is a key difference to its predecessor DNT [37]. At the time of writing, GPC is supported by the browsers Brave, DuckDuckGo, and Firefox [30].

Advanced Data Protection Control (ADPC): ADPC [39] 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 is instead customizable and allow for tailored needs. The mechanism also allows both an opt-in and opt-out approach, in contrast to the (only) 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 writing, ADPC has two prototype demo plug-ins available for Firefox and Chromium-based browsers [2].

Comparison of consent mechanisms: With P10 pointing out a browser-based consent mechanism as the preferred choice for expressing consent, we compare P3P, DNT, GPC, and ADPC to decide on a suitable baseline foundation.

Table IV shows a comparison of the browser-based consent mechanisms (P3P, DNT, GPC, and ADPC) with regards to the identified properties (P1–P10). Here, based on a manual evaluation of the documentation, we show the fulfillment measured as follows: fully fulfilled (● marker), partly fulfilled or implementation-dependent (◐), or not fulfilled (○).

In general, we see a low fulfillment 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 has been considered ambiguous as publishers can treat the GPC signals differently, as well as the signals having different meanings in different jurisdictions [37]. ADPC on the other hand aims at providing a broader privacy control, and it fulfills more of the identified evaluation properties than GPC does. Even though there are still several properties that ADPC does not fulfill (partially or not at all), we conclude that it is the existing browser-based consent mechanisms that best fulfill the full set of properties. Overall, we deem it as a suitable foundation for improvements. In this work, we use it as the basis upon which we provide suggested improvements to fulfill the remaining properties and bridge the identified privacy gaps.

B. Review of properties and suggestions for improvement

We next review each property (P1–10) from an ADPC perspective and highlight the main takeaways for the suggested improvements. Table IV summarizes the potential effect of adding these improvements (as ADPC enhancement). Here, we note that for some cases (P2, P6, and P8), even though we see improvements, the improvements are insufficient to change the property fulfillment (from partly to fully fulfilled). We note that additional improvements can be achieved through

TABLE IV. COMPARISON OF BROWSER-BASED CONSENT MECHANISMS, THE GAPS, AND EFFECTS OF POTENTIAL IMPROVEMENTS

Mechanism	Properties									
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
P3P†	◐	◐	◐	◐	◐	◐	◐	●	○	●
DNT†	○	◐	○	◐	○	○	◐	◐	○	●
GPC*	○	◐	◐	◐	○	◐	◐	◐	○	●
ADPC*	○	◐	◐	◐	◐	◐	◐	◐	○	●
ADPC enhancement	●	◐	●	●	●	◐	●	◐	●	●
Data controllers	–	●	–	–	–	●	–	–	–	–
Legislation	–	–	–	–	–	–	–	●	●	–
Combined effects	●	●	●	●	●	●	●	●	●	●

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

† = W3C official standard; * = unofficial draft

requirements from data controllers and legislation. In the table, we also include the fulfillment levels of such requirements, both when applied individually and when used in combination with our ADPC enhancements. As seen, the final combination fully closes the gaps and fulfill all properties (bottom row).

No prior storing/sending (P1): Browsers should prevent or limit storing and sending data unless there is registered consent. The user should configure the consent to allow for generality, or specific consent must be given per website. This applies to both storing and sending data. Note that data controllers should still be legally responsible for not storing and retrieving data when there is no registered consent.

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): Consent is of central importance from a legislative perspective to determine what is and what is not allowed [38]. 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)].

Websites, including the major social media websites, have been found not to use a so-called human-centric perspective of enabling informed consent, but rather to utilize patterns steering the users into consenting [38]. From a technical perspective, consenting is possibly as complex as privacy. Santos et al. [69] identified 22 legal–technical requirements for a valid consent regarding the use of cookies, with several examples of violations for each requirement.

Keeping consent within the browser prevents consent from being merged into a contract. A contract cannot overrule a usage agreed upon through specific user consent, for instance through browser settings. The website is not allowed to block access or hinder this by forcing the user into consenting to certain data sharing [69].

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 from users through "tracking walls".
Suggested improvements	(1) Add browser support for expressing consent. (2) Add browser/server support for consent withdrawal. (3) Prohibit the use of tracking or consent walls.

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

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

Informed consent (P4): Privacy information should be easily accessible, e.g., by including ADPC support within the browser interface in a standardized way. The required information would be up to the data controller to provide, and for ADPC/browser to enforce. All cookies should be documented, and the browser could prevent using 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 an important aspect that DNT failed to address. 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 website's interface. The intelligibility and use of clear and plain language are more challenging for the browser to ensure, and as such, it is up to the data controller to provide. Standardizing where the data controller provides this data also allows easy information auditing.

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 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 changing (giving and withdrawing) consent, even as a standalone 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. 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 handle, 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 is objecting. 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, e.g., information on cookies, data controllers, and rights, should be structured and made available. This is currently not solved in ADPC, even though it gives some flexibility. For browsers to easily locate the information needed, a standardized path using a well-known URI and an expansion of the ADPC consent structure would help fulfill this property.

Standardized (P8)	
Fulfillment	◐ Current ◐ Potential
Requirement	The location of required information needs to be standardized, and the structure for the 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 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 needed from a legal standpoint, but to a large extent, GDPR is already clear on what is included in legitimate interest. To support transparency, all cookies should be motivated and explained, even those considered necessary

or allowed based on legitimate interest. By utilizing the same standardized approach as suggested by P8, necessary cookies can include a `Necessary` attribute and be allowed to be used pre-approved only by ensuring that all data is complete. This would allow for broad scale auditing of websites to reveal any misuse of trust and thus possible to blocklist or similar. For example, necessary cookies could include settings such as language, layout, or dark mode, as well as active log-in action to keep the 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 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 mentions technical settings 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 *Article 29 Working Party* (WP29) has written extensively about the requirement for consent, stating browser settings as a way to obtain consent [8]. The data controller must be *"confident that the user has been fully informed and actively configured their browser or other application"* [8]. 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"* [7]. WP29 notes that it is important that browsers are provided with default privacy-protective settings, adding that browsers should have privacy wizards upon first installation/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 using 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 suggestions of P1–P9.

IV. Putting it all together

We next combine the suggested improvements into an improved version of ADPC that we call ADPC+ and describe how ADPC+ can be implemented and put to use. First, we present five concrete features that together make up the improvements of ADPC+ and evaluate the resulting property fulfillment. Then, we review the involvement of the parties, discuss incentives, and propose an implementation roadmap capturing feature dependencies and division of responsibilities.

A. Suggested features

Table V summarizes the five distinct features proposed, shows the stakeholders responsible for the implementation, and discusses the requirements to fulfill the intended properties. We note that these presented features can be implemented either as standalone features or as part of a new standard.

TABLE V. Overview of the suggested features and implementation requirements for involved parties

Feature	Responsible	Implementation
F1	Browser software	✓ Blocking of storing/sending data prior to consent.
	Server software	-
	Data controller	-
F2	Browser software	✓ 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 controller	✓ Provide all the required privacy, consent, and cookie information in the given well-known location. ✓ Ensure clear, plain, and understandable language. Preferably in all target-audience languages.
F3	Browser software	✓ Interface for giving and withdrawing consent, in connection with information in Feature 2. ✓ Signaling to send and monitor consent withdrawal.
	Server software	✓ Support for consent withdrawal and forwarding.
	Data controller	✓ Ensure correct handle of all consent withdrawals. ✓ Do not utilize tracking or consent walls.
F4	Browser software	✓ Support for ADPC header fields. ✓ Support for sending/retrieving consent requests.
	Server software	✓ Support for ADPC header fields. ✓ Support for sending/retrieving consent requests.
	Data controller	-
F5	Browser software	✓ Support for determining necessary cookies and uses. ✓ Only allow necessary cookies without consent.
	Server software	-
	Data controller	✓ Provide complete information according to Feature 2 on all necessary cookies. ✓ Do not abuse the use of necessary—it is legally enforceable.

No prior storing/sending of data (F1): This first feature primarily fulfills P1 and is implemented in the browser. Browsers should only accept storing and sending cookie data and similar if there is a registered specific (per website and purpose) consent configured by the user (handled by Feature 2). The only exception to this rule is necessary cookies, as specified in Feature 5 according to P9.

Present complete and required information (F2): This feature involves a shared responsibility between the browser software and the data controllers. Here, browsers provide a standardized interface populated with data from the data controller. When a user visits a website, the browser loads the information from the server, displays it in the dedicated interface, and notifies the user. As an effect, 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+.

Well-Known *Uniform Resource Identifiers* (URIs) [63] are special URIs reserved for data related to a resource origin. Here, all information required from the data controller should be located in a well-known location such as the host URI followed by `/.well-known/privacy` or `/.well-known/adpc`. The data should include at least 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 in which the information is available, and the information could then be located using an ISO country–language standard suffix, e.g., en_US.

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.

Configurable and changeable specific consent per purpose (F3): 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 purpose 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. Furthermore, 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 described as Feature 4.

Browser–server and server–server communication (F4): To support Feature 3 and possible 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 controllers.

An `ADPC` header is already used in the current ADPC draft, including for withdrawing consent. Expanding on this would be preferred. 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 confirmed, a withdrawal 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 [25] 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.

Require consent for cookies without `Necessary` attribute (F5): 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. 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 allows for semi-automated auditing, where servers can be queried to retrieve a list of necessary cookies and purposes that can be reviewed.

B. Property fulfillment

Combining the presented features, ADPC+ bridges the gaps and explicitly address most of the desirable properties. Table VI shows all features with their contribution mapped to each property, the responsible implementation parties, and the resulting property fulfillment of ADPC+.

We note that the suggested features only partially solve P8 (Standardized). While the features solve the technical standardization, more guidance is needed from legislation regarding pre-defined purposes and similar. Furthermore, the features cannot fully ensure P2 (Freely given consent) and P6 (Readable and accessible), as there are still ways for data controllers to force users to give consent and to provide incomplete or otherwise non-compliant information. However, as previously shown in Table IV, the proposed properties are fully fulfilled when combined with legislation and data controller compliance. ADPC+ thus satisfies the set-out goals.

C. Incentives and effects on affected parties

Technical implementers: In the age of GDPR and CCPA, user privacy is a competitive advantage. Not only are an

TABLE VI. SUGGESTED FEATURES, IMPLEMENTATION RESPONSIBILITY, AND PROPERTY FULFILLMENT

Features	Implementation			Property fulfillment									
ADPC feature additions	Browser	Server	Data cont.	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 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

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. The initiatives already taken by major browsers show that privacy is high 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 add additional protective features based on those to limit data sharing, this would be an enormous benefit for the user and provide a strong incentive to switch to a more privacy-aware browser.

For servers, the incentive boils down to compliance with web standards, which ADPC+ would potentially qualify. In the meantime, plugins for ADPC+ server support could be developed that both website owners and data controllers can utilize. This would incentivize service providers to use plugins until the server software vendors offer native support.

Data controllers: One notable effect of the suggested features is an increased burden on data controllers. However, some (if not all) that 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 the data controller.

From an incentive perspective, legal compliance might be the most prominent one. The potential economic blow of being fined for GDPR non-compliance is a strong motivator. There are, of course, also data controllers that are self-motivated to show a strong respect for user privacy and thus would have incentive to showcase ADPC+ compliance. With more privacy awareness, data subjects might be more likely to choose websites that respect user privacy in the future. Also, websites may therefore come to see ADPC+ compliance as a way to showcase their respect for user privacy, providing further incentive to comply.

Data subjects: Finally, the reason all privacy legislation has been established, namely data subjects. The effect on data subjects is of central importance in the suggested improvements and is the primary reason they are needed. Implementing the suggested features would create notably enhanced user privacy and data control, and provide strong incentives for data controllers to comply, effectively creating a positive snowball effect of user privacy enhancement.

We acknowledge that the need to configure browser settings might unavoidably worsen the user experience for some, especially those having utilized content blockers before to remove notices and cookie banners. However, this is a small price to increase user privacy, and also necessary 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 today's cookie banner configuration overhead.

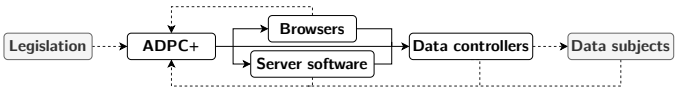

Fig. 1. Overview of the implementation dependencies and influences

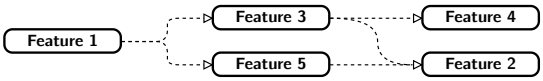

Fig. 2. Overview of the feature dependencies

D. Implementation roadmap

ADPC+ can be incrementally implemented and deployed. Here, we outline our suggested implementation roadmap. At a high level, the roadmap begins with adding the proposed features (F1–F5) to the existing ADPC standard. Once standardized, browsers and server software can implement support for ADPC+ (and its features) for data controllers. As data controllers provide the required information, the data subject's browser experience will improve as more features are being implemented and the standards increasingly are being adopted and adhered to. Figure 1 illustrates the dependencies and influences in the suggested implementation process.

With legislation being the main driver to improve user privacy, we note that the suggested features are based on the current European legislative landscape. While this also explains why the implementation process starts with ADPC+, we must also note that the primary foundation for further enhancements to ADPC will be legislation and 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 involve the ADPC community creating an enhanced draft. For ADPC+ to reach a broad audience and become a broadly accepted standard, standardization bodies such as the W3C and the Internet Engineering Task Force (IETF) would need to be involved. No matter the scenario, documentation of the ADPC enhancements must be completed before other stakeholders can begin their work.

Table VI also includes 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+ depend on browser implementations, and there are two ways to achieve this. The first way is through the current (prototype) variant, creating plugins for browsers that add the needed functionality. The second way, described next, is preferred. Here, the browser vendor instead implements the functionality as part of the browser. In this case, both the browser's user interface and the engine must implement features to fulfill the requirements. To ensure compliance, the latter would need to be developed alongside the server software.

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

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

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

Figure 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 depends on having the required information, offered by Feature 2, and withdrawing consent through browser–server and server–server communication, offered by Feature 4. Feature 5 depends on Feature 2 to provide functionality for `Necessary`.

We see here that Features 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, Features 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 is not desirable. A cohesive and coordinated implementation between all parties is strongly preferable to create an environment for compliance.

V. Related work

Online user privacy: Several ways that (unethical) entities may track users have been studied, including the use of browser fingerprinting or mobile tracking. Using browser fingerprint, content providers can uniquely identify browser instances without the need to use cookies [52]. Because of its nature, bypassing user consent and ability to decline, the technique violates GDPR and is more challenging to prevent or mitigate. Papadogiannakis et al. [66] look at how websites bypass GDPR consent, concluding that 75% of tracking activities happen before users can provide consent or choose to reject. Other works have studied users' perspectives on fingerprinting, including how to protect themselves [35], [36], [67].

As new protocols arise, fingerprinting might (at least temporarily) be more challenging, as shown by Smith et al. [73] in a study where QUIC is fingerprinted with TCP-trained classifiers. Other related works include formal models of data sharing [86] and comparisons of web tracking on mobile and desktop environments [93]. User awareness, adoption of, and misconceptions of web privacy tools is also a closely related area previously studied [77]. Additional perspectives on privacy notices are how privacy can be enhanced through design [46] and additional effects after GDPR [53]. One emerging trend of recent years is to use machine learning for interpreting privacy policies [5], [13], [43].

Some tracking prevention techniques having been deployed by browser vendors include the *Intelligent Tracking Prevention* (ITP) [6] initiative in Safari, and *Enhanced Tracking Protection* (ETP) [61] in Firefox. Other web initiatives include ad, script, tracking, and content blockers. However, as these infer with the website, they can be detectable and can trigger websites to nudge for inactivation or to block the requested content from being served [58]. Ad blockers can also be deceiving. Smullen et al. [74] show that when ads were not present, users falsely assume that there are no potentially intrusive practices.

Finally, previous works have studied technical standards for CCPA [37], [65], [95] and the legal effects of GDPR before the final version was approved [14]. There are also more dimensions of online privacy than cookies, including a proposal to enhance privacy for TLS over TCP Fast Open [79].

Undisclosed and non-web tracking: Tracking in apps is also an emerging area of interest. Han et al. [34] compare the privacy in free and paid apps, finding that paid apps use the same third-party libraries and permissions as their free counterparts. Kollnig et al. [47] show that most apps use third-party tracking, but only a few obtained valid consent before tracking. There have also been initiatives to find universal guidelines for displaying and using consent dialogs [23]. Major organizations are also working towards preventing undisclosed tracking in apps. For example, Apple's *App Tracking Transparency* (ATT) policy requires developers to explicitly ask for permission when using information from other companies' apps [58].

Privacy has also been considered in many other closely related domains, including Internet of Things, where access control policies and privacy preference languages have been proposed [9], [88]. Privacy policies have also been extensively studied and proposed in areas outside the web, such as for health and other more general appliances [21], [32], [57]. From a developer perspective, there have been studies specifically nudging developers about user privacy [80], and the development of privacy design patterns based on privacy principles and UML [78].

Policy languages: There have been many initiatives within the area of consent, transparency, and privacy, with several policy languages presented [11], [42], [45], [60], [94] and initiatives to enforce them [1]. Similar to the legal foundation in this work, there has been previous research in the

interdisciplinary legal–technical domain seeking to technically bridge the legal challenges [51]. Additional proposals have also been presented in the light of GDPR [10], [29]. Furthermore, the policy-aware web is a notable initiative aimed at creating a rule-based policy management system and building on the semantic web [91], [92]. A recent example seeks to create a systematization of longitudinal privacy management [72].

VI. Conclusion

In this paper, we have presented a browser-based consent framework, ADPC+, that incorporates five features motivated by privacy gaps and mechanism properties identified based on the literature. First, we have addressed the current challenges and requirements of user privacy control. Here, we proposed ten properties needed to bridge the privacy gap. Expanding on previous work, we identified standardization, the distinction between necessary and unnecessary cookies, and technical enforcement of consent through browser mechanisms as additional properties of an ideal solution. Second, we have studied how browser-based consent mechanisms may provide conditions for legal compliance. Motivated by GDPR and WP29, the suggested features showcase how valid consent can be expressed through browser settings and thus provide conditions for legal compliance. Finally, we have presented five concrete features of browser-based consent mechanisms that are required to bridge the current gaps and provided an implementation roadmap of ADPC+.

While implementing a prototype solution and the five features (based on ADPC) using plugins remains future work, we have provided a well-motivated foundation together with an implementation roadmap. If adopted, we expect ADPC+ to provide a big step towards finally simultaneously achieving seamless browsing and informed consent.

Acknowledgment

This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

References

[1] C. Adams, Y. Dai, C. DesOrmeaux, S. McAvoy, N. Nguyen, and F. Trindade, "Strengthening enforcement in a comprehensive architecture for privacy enforcement at internet websites," *Frontiers in Computer Science*, 2020.

[2] Advanced Data Protection Control (ADPC), https://www.dataprotectioncontrol.org/prototype/, 2022.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "An XPath-based preference language for P3P," in *Proc. World Wide Web Conference (WWW)*, 2003.

[4] ——, "XPref: a preference language for P3P," *Computer Networks*, 2005.

[5] A. Alabduljabbar, A. Abusnaina, U. Meteriz-Yildiran, and D. Mohaisen, "TLDR: Deep learning-based automated privacy policy annotation with key policy highlights," in *Proc. ACM CCS Workshop on Privacy in the Electronic Society (WPES)*, 2021.

[6] Apple, "Tracking prevention in WebKit," https://webkit.org/tracking-prevention/, 2022.

[7] Article 29 Data Protection Working Party, "Opinion 2/2010 on online behavioural advertising," European Commission, Tech. Rep. 00909/10/EN WP 171, 2010. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

[8] ——, "Working document 02/2013 providing guidance on obtaining consent for cookies," European Commission, Tech. Rep. 1676/13/EN WP 208, 2013. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[9] H. F. Atlam, M. O. Alassafi, A. Alenezi, R. J. Walters, and G. B. Wills, "XACML for building access control policies in internet of things," in *Proc. Internet of Things, Big Data and Security (IoTBDS)*, 2018.

[10] S. Becher, A. Gerl, and B. Meier, "Don't forget the user: From user preferences to personal privacy policies," in *Proc. Advanced Computer Information Technologies (ACIT)*, 2020.

[11] M. Becker, A. Malkis, and L. Bussard, "A framework for privacy preferences and data-handling policies," Microsoft Research, Tech. Rep. MSR-TR-2009-128, 2009.

[12] R. Berjon, S. Zimmeck, A. Soltani, D. Harbage, and P. Snyder, "Global Privacy Control (GPC)," Proposal, Tech. Rep., 2022. [Online]. Available: https://globalprivacycontrol.github.io/gpc-spec/

[13] D. Bui, K. G. Shin, J.-M. Choi, and J. Shin, "Automated extraction and presentation of data practices in privacy policies," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2021.

[14] D. Butin and D. Le Métayer, "A guide to end-to-end privacy accountability," in *Proc. IEEE/ACM Workshop on Technical and Legal Aspects of Data Privacy and Security (TELERISE)*, 2015.

[15] J. Castiglione, D. Pavlovic, and P.-M. Seidel, "Privacy protocols," *Foundations of Security, Protocols, and Equational Reasoning*, 2019.

[16] R. Chen, F. Fang, T. Norton, A. M. McDonald, and N. Sadeh, "Fighting the fog: Evaluating the clarity of privacy disclosures in the age of CCPA," in *Proc. ACM CCS Workshop on Privacy in the Electronic Society (WPES)*, 2021.

[17] L. Cranor, M. Langheinrich, and M. Marchiori, "A P3P preference exchange language 1.0 (APPEL1.0)," W3C, Tech. Rep., 2004. [Online]. Available: https://www.w3.org/TR/2002/WD-P3P-preferences-20020415/

[18] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, "The platform for privacy preferences 1.0 (P3P1.0) specification," W3C, Tech. Rep., 2018. [Online]. Available: https://www.w3.org/TR/2018/OBSL-P3P-20180830/

[19] L. F. Cranor, "P3P: Making privacy policies more useful," *IEEE Security Privacy*, 2003.

[20] F. Debusseré, "The EU e-privacy directive: A monstrous attempt to starve the cookie monster?" *International Journal of Law and Information Technology*, 2005.

[21] H. DeYoung, D. Garg, L. Jia, D. Kaynar, and A. Datta, "Experiences in the logical specification of the HIPAA and GLBA privacy laws," in *Proc. ACM CCS Workshop on Privacy in the Electronic Society (WPES)*, 2010.

[22] N. Doty, H. West, J. Brookman, S. Harvey, and E. Newland, "Tracking compliance and scope," W3C, Tech. Rep., 2019. [Online]. Available: https://www.w3.org/TR/2019/NOTE-tracking-compliance-20190122/

[23] A. P. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. Wagner, "How to ask for permission," in *Proc USENIX Workshop on Hot Topics in Security (HotSec)*, 2012.

[24] R. Fielding, "Apache does not tolerate deliberate abuse of open standards," https://github.com/apache/httpd, 2012.

[25] R. Fielding and J. Reschke, "Hypertext transfer protocol (HTTP/1.1): Semantics and content," RFC 7231, 2014.

[26] R. Fielding and D. Singer, "Tracking preference expression (DNT)," W3C, Tech. Rep., 2019. [Online]. Available: https://www.w3.org/TR/2019/NOTE-tracking-dnt-20190117/

[27] G. Fleishman, "How the tragic death of Do Not Track ruined the web for everyone," https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone, 2019.

[28] I. Fouad, C. Santos, F. Al Kassar, N. Bielova, and S. Calzavara, "On compliance of cookie purposes with the purpose specification principle," in *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2020.

[29] A. Gerl, N. Bennani, H. Kosch, and L. Brunie, "LPL, towards a GDPR-compliant privacy language: Formal definition and usage," *Trans. on Large-Scale Data- and Knowledge-Centered Systems XXXVII*, 2018.

[30] Global Privacy Control (GPC), https://globalprivacycontrol.org/, 2022.

[31] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark patterns and the legal requirements of consent banners: An interaction criticism perspective," in *Proc. ACM Human Factors in Computing Systems (CHI)*, 2021.

[32] W. Guo, J. Rodolitz, and E. Birrell, "Poli-See: An interactive tool for visualizing privacy policies," in *Proc. ACM CCS Workshop on Privacy in the Electronic Society (WPES)*, 2020.

[33] H. Habib, M. Li, E. Young, and L. Cranor, "'Okay, Whatever': An evaluation of cookie consent interfaces," in *Proc. ACM Human Factors in Computing Systems (CHI)*, 2022.

[34] C. Han, I. Reyes, Álvaro Feal, J. Reardon, P. Wijesekera, N. Vallina-Rodriguez, A. Elazari, K. A. Bamberger, and S. Egelman, "The price is (not) right: Comparing privacy in free and paid apps," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2020.

[35] D. Hasselquist, M. Lindblom, and N. Carlsson, "Lightweight fingerprint attack and encrypted traffic analysis on news articles," in *Proc. IFIP Networking*, 2022.

[36] D. Hasselquist, C. Vestlund, N. Johansson, and N. Carlsson, "Twitch chat fingerprinting," in *Proc. IFIP Network Traffic Measurement and Analysis Conference (TMA)*, 2022.

[37] M. Hils, D. W. Woods, and R. Böhme, "Privacy preference signals: Past, present and future," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2021.

[38] S. Human and F. Cech, "A human-centric perspective on digital consenting: The case of GAFAM," in *Proc. Human Centred Intelligent Systems (HCIS)*, 2021.

[39] S. Human, M. Schrems, A. Toner, Gerben, and B. Wagner, "Advanced data protection control (ADPC)," WU Vienna University of Economics and Business, Tech. Rep., 2021.

[40] IAB Europe, "TCF - Transparency & consent framework," https://iabeurope.eu/transparency-consent-framework/.

[41] Information Commissioner's Office, "ICO to call on G7 countries to tackle cookie pop-ups challenge," 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/, 2021.

[42] S. Kasem-Madani and M. Meier, "Security and privacy policy languages: A survey, categorization and gap identification," 2015.

[43] R. Khandelwal, T. Linden, H. Harkous, and K. Fawaz, "PriSEC: A privacy settings enforcement controller," in *Proc. USENIX Security*, 2021.

[44] S. Khodayari and G. Pellegrino, "The state of the SameSite: Studying the usage, effectiveness, and adequacy of SameSite cookies," in *Proc. IEEE Symposium on Security and Privacy (S&P)*, 2022.

[45] S. Kirrane, J. D. Fernández, W. Dullaert, U. Milosevic, A. Polleres, P. A. Bonatti, R. Wenning, O. Drozd, and P. Raschke, "A scalable consent, transparency and compliance architecture," in *Proc. European Semantic Web Conference (ESWC)*, 2018.

[46] A. Kitkowska, M. Warner, Y. Shulman, E. Wästlund, and L. A. Martucci, "Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect," in *Proc. USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2020.

[47] K. Kollnig, R. Binns, P. Dewitte, M. V. Kleek, G. Wang, D. Omeiza, H. Webb, and N. Shadbolt, "A Fait Accompli? An empirical study into the absence of consent to third-party tracking in android apps," in *Proc. USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2021.

[48] M. Kretschmer, J. Pennekamp, and K. Wehrle, "Cookie banners and privacy policies: Measuring the impact of the GDPR on the web," *ACM Trans. on the Web*, 2021.

[49] C. Krisam, H. Dietmann, M. Volkamer, and O. Kulyk, "Dark patterns in the wild: Review of cookie disclaimer designs on top 500 German websites," in *Proc. European Symposium on Usable Security (EuroUSEC)*, 2021.

[50] L. Kyi, S. Ammanaghatta, F. Roesner, C. Santos, F. Zufall, and A. J. Biega, "Investigating deceptive design in GDPR's legitimate interest," in *Proc. ACM Conference on Human Factors in Computing Systems (CHI)*, 2023.

[51] D. Le Métayer, "A formal privacy management framework," in *Proc. Formal Aspects in Security and Trust (FAST)*, 2009.

[52] S. Li and Y. Cao, "Who touched my browser fingerprint? A large-scale measurement study and classification of fingerprint dynamics," in *Proc. ACM Internet Measurement Conference (IMC)*, 2020.

[53] T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz, "The privacy policy landscape after the GDPR," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2020.

[54] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems: A user study of consent dialogs after GDPR," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2020.

[55] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice? : Measuring legal compliance of banners from IAB Europe's transparency and consent framework," in *Proc. IEEE Symposium on Security and Privacy (S&P)*, 2020.

[56] C. Matte, C. Santos, and N. Bielova, "Purposes in IAB Europe's TCF: Which legal basis and how are they used by advertisers?" in *Proc. Privacy Technologies and Policy*, 2020.

[57] M. J. May, C. A. Gunter, and I. Lee, "Privacy APIs: access control techniques to analyze and verify legal privacy policies," in *Proc. IEEE Computer Security Foundations Workshop (CSFW)*, 2006.

[58] M. Mehrnezhad, K. Coopamootoo, and E. Toreini, "How can and would people protect from online tracking?" in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2022.

[59] Microsoft, "P3P is no longer supported," https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/mt146424(v=vs.85), 2016.

[60] V. Morel and R. Pardo, "SoK: Three facets of privacy policies," in *Proc. ACM CCS Workshop on Privacy in the Electronic Society (WPES)*, 2020.

[61] Mozilla, "Enhanced tracking protection in firefox for desktop," https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop, 2022.

[62] D. Napoli, K. Baig, S. Maqsood, and S. Chiasson, "I'm literally just hoping this will work: Obstacles blocking the online security and privacy of users with visual disabilities," in *Proc. USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2021.

[63] M. Nottingham, "Well-known uniform resource identifiers (URIs)," RFC 8615, 2019.

[64] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence," in *Proc. ACM Human Factors in Computing Systems (CHI)*, 2020.

[65] S. O'Connor, R. Nurwono, A. Siebel, and E. Birrell, "(Un)Clear and (In)Conspicuous: The right to opt-out of sale under CCPA," in *Proc. ACM CCS Workshop on Privacy in the Electronic Society (WPES)*, 2021.

[66] E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, and E. P. Markatos, "User tracking in the post-cookie era: How websites bypass GDPR consent to track users," in *Proc. Web Conference (WWW)*, 2021.

[67] G. Pugliese, C. Riess, F. Gassmann, and Z. Benenson, "Long-term observation on browser fingerprinting: Users' trackability and perspective," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2020.

[68] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, and I. Santos, "Can i opt out yet? GDPR and the global illusion of cookie control," in *Proc. ACM Asia Conference on Computer and Communications Security (Asia CCS)*, 2019.

[69] C. Santos, N. Bielova, and C. Matte, "Are cookie banners indeed compliant with the law?" *Technology and Regulation*, 2020.

[70] C. Santos, M. Nouwens, M. Toth, N. Bielova, and V. Roca, "Consent management platforms under the GDPR: Processors and/or controllers?" in *Proc. Privacy Technologies and Policy*, 2021.

[71] C. Santos, A. Rossi, L. Sanchez Chamorro, K. Bongard-Blanchy, and R. Abu-Salma, "Cookie banners, what's the purpose? Analyzing cookie banner text through a legal lens," in *Proc. ACM CCS Workshop on Privacy in the Electronic Society (WPES)*, 2021.

[72] T. Schnitzler, S. Mirza, M. Dürmuth, and C. Pöpper, "SoK: Managing longitudinal privacy of publicly shared personal online data," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2021.

[73] J.-P. Smith, P. Mittal, and A. Perrig, "Website fingerprinting in the age of QUIC," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2021.

[74] D. Smullen, Y. Yao, Y. Feng, N. Sadeh, A. Edelstein, and R. Weiss, "Managing potentially intrusive practices in the browser: A user-centered perspective," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2021.

[75] State of California Department of Justice Attorney General, "California consumer privacy act regulations," https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf, 2018.

[76] ——, "California Consumer Privacy Act (CCPA)," https://oag.ca.gov/privacy/ccpa, 2022.

[77] P. Story, D. Smullen, Y. Yao, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub, "Awareness, adoption, and misconceptions of web privacy tools," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2021.

[78] T. Suphakul and T. Senivongse, "Development of privacy design patterns based on privacy principles and UML," in *Proc. IEEE/ACIS Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2017.

[79] E. Sy, T. Mueller, C. Burkert, H. Federrath, and M. Fischer, "Enhanced performance and privacy for TLS over TCP Fast Open," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2020.

[80] M. Tahaei, A. Frik, and K. Vaniea, "Deciding on personalized ads: Nudging developers about user privacy," in *Proc. USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2021.

[81] J. Tang, H. Shoemaker, A. Lerner, and E. Birrell, "Defining privacy: How users interpret technical terms in privacy policies," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2021.

[82] The Electronic Frontier Foundation, "A privacy-friendly do not track (DNT) policy," https://www.eff.org/dnt-policy, 2018.

[83] The European Parliament and the Council of the European Union, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," 2002.

[84] ——, "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," 2009.

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

[86] G. D. Tizio and F. Massacci, "A calculus of tracking: Theory and practice," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2021.

[87] M. Trevisan, S. Traverso, E. Bassi, and M. Mellia, "4 years of EU cookie law: Results and lessons learned," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2019.

[88] M.-R. Ulbricht and F. Pallas, "YaPPL - A lightweight privacy preference language for legally sufficient and automated consent provision in IoT scenarios," in *Proc. Data Privacy Management, Cryptocurrencies and Blockchain Technology (CBT)*, 2018.

[89] United Nations General Assembly, "Universal declaration of human rights," https://www.un.org/sites/un2.un.org/files/udhr.pdf, 1948.

[90] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)Informed consent: Studying GDPR consent notices in the field," in *Proc. ACM Computer and Communications Security (CCS)*, 2019.

[91] D. J. Weitzner, H. Abelson, T. Berners-Lee, C. Hanson, J. Hendler, L. Kagal, and G. J. Sussman, "Transparency and end-to-end accountability: Requirements for web privacy policy languages," in *Proc. W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*, 2006.

[92] D. J. Weitzner, J. Hendler, T. Berners-Lee, and D. Connolly, "Creating the policy-aware web: Discretionary, rules-based access for the world wide web," *Web and Information Security*, 2006.

[93] Z. Yang and C. Yue, "A comparative measurement study of web tracking on mobile and desktop environments," in *Proc. Privacy Enhancing Technologies (PoPETs)*, 2020.

[94] J. Zhao, R. Binns, M. Van Kleek, and N. Shadbolt, "Privacy languages: Are we there yet to enable user controls?" in *Proc. Companion on World Wide Web (WWW)*, 2016.

[95] S. Zimmeck and K. Alicki, "Standardizing and implementing do not sell," in *Proc. ACM CCS Workshop on Privacy in the Electronic Society (WPES)*, 2020.