Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges

Soheil Human*†, Harshvardhan J. Pandit‡, Victor Morel*, Cristiana Santos§, Martin Degeling¶, Arianna Rossi‖, Wilhelmina Botes‖, Vitor Jesus**, Irene Kamara††

* *Institute for Information Systems and New Media, Vienna University of Economics and Business, Vienna, Austria*

† *Department of Philosophy & Vienna Cognitive Science Hub, University of Vienna, Vienna, Austria*

‡ *ADAPT Centre, Trinity College Dublin, Dublin, Ireland*

§ *Universiteit Utrecht, Utrecht, Netherlands*

¶ *Ruhr University Bochum, Bochum, Germany*

‖ *SnT Interdisciplinary Centre for Security Reliability and Trust, University of Luxembourg, Luxembourg*

** *Aston Business School, Aston University, Birmingham, UK*

†† *Tilburg Law School, Tilburg University, Tilburg, Netherlands*

Corresponding Author: soheil.human@wu.ac.at — soheil.human@univie.ac.at

Abstract

Data Protection and Consenting Communication Mechanisms (DPCCMs) enable users to express their privacy decisions and manage their online consent. Thus, they can become a crucial means of protecting individuals' online privacy and agency, thereby replacing the current problematic practices such as "consent dialogues". Based on an in-depth analysis of different DPCCMs, we propose an interdisciplinary set of factors that can be used for a comparison of such mechanisms. Moreover, we use the results from a qualitative expert study to identify some of the main multidisciplinary challenges that DPCCMs should address to become widely adopted data privacy mechanisms. We leverage both the factors and the challenges to compare two current *open specifications*, i.e. the Advanced Data Protection Control (ADPC) and the Global Privacy Control (GPC), and discuss future work.

1. Introduction

The increasing adoption of online technologies has caused serious concerns regarding data privacy and users' agency (see e.g. [1]), as they expose both individuals and societies to several risks: from the implementation of so-called *dark patterns* that extort consent to personal data processing [2]–[4], through direct marketing meant to sway political elections [5], to other forms of online influence that cause the systemic socioeconomic upheaval of our societies [6]. Addressing such concerns to protect individual and collective rights has caused one of the most challenging interdisciplinary endeavours of our time. One way to address these concerns is to consider Human-centric, Accountable, Lawful, and Ethical (HALE) [7] manners to communicate data, metadata, information, user preferences, or decisions regarding personal data processing, and assisting end-users to express their privacy decisions through free and informed consent [8] implemented by novel sociotechnical means [9]. However, the current *web-based data processing mechanisms* still lack effective underlying mechanisms that provide such functionalities. *Data Protection and Consenting Communication Mechanisms* (DPCCMs), also known as *privacy automated signals* [1], are meant to address some of these issues, namely the lack of communication mechanisms between data controllers and data subjects. Historically, *privacy signals* were used to refer to some of these mechanisms. However, considering 1) the intersectionality of data protection consent and other types of *consent* [2], and 2) the fact that such mechanisms can potentially go beyond simple signals (e.g. binary signals) and become *advanced mechanisms using diverse technologies*, we deliberately adopt the term Data Protection and Consenting Communication Mechanisms (DPCCMs). As it is evident from their names, DPCCMs are mechanisms that can be used for the communication of data, metadata, information, preferences, or/and decisions related to data protection or/and consenting between different actors. They vary in their approach and ambition, and range from simple *binary signals* such as the "Do Not Track"[3] (DNT) and the more recent "Global Privacy Control"[4] (GPC) [11], to more *expressive* mechanisms such as the Platform for Privacy Preferences Project (P3P)[5], the "Advanced Data Protection Control"[6] (ADPC) [12], [13], and industry-controlled efforts such as the IAB Europe Transparency and Consent Framework[7] (TCF v2). Earlier attempts, such as DNT and P3P, faced strong multidimensional barriers to their adoption and a lack of legal enforcement, which led them to rapidly become obsolete [14]. However, DPCCMs have seen a resurgence in recent times (i.e., GPC, ADPC, TCF), owing to multiple factors: advancements in data protection and

1. The two terms are used interchangeably in the paper.

2. Consent is not always limited to privacy, hence the term "*privacy* signal" does not cover other types of consents that can/must be communicated [10], for instance biomedical consent.

3. https://www.w3.org/TR/tracking-dnt/

4. https://globalprivacycontrol.github.io/gpc-spec/

5. https://www.w3.org/TR/P3P11/

6. https://www.dataprotectioncontrol.org/spec/

7. https://iabeurope.eu/tcf-2-0/

privacy legislation, in particular the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA); and proactive measures taken by large platforms such as Apple's App Tracking Transparency (ATT) [8]. Considering the importance of DPCCMs and the lack of comparative research on current proposals, after a short presentation of the two main open proposals in Section 2 and a description of the methodology used in Section 3, this paper presents a study investigating four research questions: (**RQ1**) *What are the technical factors that can be used to characterize and compare DPCCMs?* (**RQ2**) *What are the differences between the current open-standard DPCCM proposals (GPC and ADPC) based on the identified technical factors?* The answers to these first two questions are illustrated in Section 4. (**RQ3**) *What are the challenges to realize a Human-centric, Accountable, Lawful, and Ethical DPCCM?* is answered in Section 5. Finally, Section 6 tackles the last research question: (**RQ4**) *To what extent are the identified challenges addressed in the current GPC and ADPC proposals?* Section 7 concludes the work.

2. Current Proposals: GPC and ADPC

We focus on GPC and ADPC, since the other proposals (e.g., TCF and ATT) are: (i) not open specifications that can be implemented by anyone; (ii) strictly regulated within a limited context (e.g. use by companies); or (iii) in the case of TCF, arguably insufficient to meet legal requirements by design [15].

Global Privacy Control (GPC). GPC is a unary signal similar to DNT. Whereas DNT specifies binary values to permit or prohibit [third-party] tracking, GPC has a single state expressing "Do Not Sell". Like DNT, GPC is communicated by the user-agent through HTTP headers or DOM, and is enforceable as a "user-enabled global privacy control" under the California Consumer Privacy Act (CCPA 999.315). As of January 2022, GPC has been implemented by several actors, such as web-browsers (e.g., Brave, DuckDuckGo, Firefox) and popular websites (e.g., New York Times, Washington Post), with support expressed by Consent Management Providers (CMP) like OneTrust and TrustArc. The GPC specification might have potential application to other jurisdictions, e.g. to be employed to "limit the sale or sharing" of personal data based on GDPR's Article 7 (Conditions for consent) and Article 21 (Right to object). However, this is a matter of further investigation and discussions, as the GPC is not specifically designed to correspond to EU regulations and any correlations made to the GDPR are explicitly mentioned in the GPC text as experimental.

Advanced Data Protection Control (ADPC). ADPC, similar to P3P, is a bidirectional communication mechanism that can be initiated by either websites or users. It can express multiple distinct values regarding the purposes for which consent is given or withheld, and can object to direct marketing and legitimate interest. ADPC can be communicated using HTTP headers, DOM, or a JavaScript API. It was developed as part of the RESPECTED project, [9] led by Soheil Human (Sustainable Computing Lab of the Vienna University of Economics and Business) and Max Schrems (NOYB – European Center for Digital Rights). [10] ADPC specifies its intended application for the EU Charter of Fundamental Rights' Article 8 (and Article 3), GDPR's Recital 32 and Article 7, Article 21, and ePrivacy Directive's Recital 32 (Use of user-agent), and may be used as an automated communication mechanism under the proposed ePrivacy Regulation [11].

3. Methodology

To answer our research questions, we first reviewed and analysed the technical specifications and documents related to P3P, DNT, GPC, ADPC, TCF, NAI [12], GAID [13], and ATT. Based on this document analysis, a technical comparison of factors (reported in Section 4) was performed (**RQ1**). While such factors can contribute to describe and compare different types of DPCCMs in the future, here we used them to compare GPC and ADPC (**RQ2**). We then carried out online multimodal semi-structured focus groups. These groups, comprised of the co-authors of this paper, included eight privacy experts (with gender balance) working at seven different academic institutions: three computer scientists (one web privacy expert, one IoT privacy expert, one data security expert), two privacy HCI experts, two lawyers (experts in data protection), and one expert in privacy standards, besides the moderator with a background in cognitive science, information systems, and sociology of technology. The focus groups iterated along several three hours sessions, where the participants simultaneously worked on an online whiteboard and joined an online call, thereby providing multimodal (textual, visual and verbal) inputs. The data was analysed based on a grounded theory approach [16], with three rounds of coding, and the experts validated the reported results regarding the main challenges that DPCCMs entail (**RQ3**, reported in Section 5 and **RQ4**, reported in Section 6).

4. Technical Comparison of GPC & ADPC

The technical factors of GPC and ADPC are presented in Table 1 and classified into 1) the content of the signals, 2) their possible interpretation, 3) their means of communication, and 4) the contextual factors.

8. https://developer.apple.com/documentation/apptrackingtransparency

9. https://www.respected.eu/

10. *One of the nine authors of this paper was directly involved in the development of the ADPC.*

11. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

12. https://optout.networkadvertising.org/?c=1

13. https://support.google.com/googleplay/android-developer/answer/6048248?hl=en

4.1. Signal Contents

4.1.1. Captured Intent. This relates to the *intent* or *action* of the user that the signal represents and conveys in terms of permissions and prohibitions. For example, it can specify and communicate the user's intention to opt-in or opt-out. Both GPC (for *sale of data*) and ADPC (for *indicated purposes*) support opt-out intentions by declaring prohibitions, while ADPC also supports opt-in (for indicated purposes).

4.1.2. Extensibility. This refers to the ability of adding and/or changing information in the signal's communication while adhering to its specification. It is meant to extend its use to additional values, use-cases, or contexts other than those it was developed for. GPC does not define mechanisms through which it can be extended, while ADPC does, as it allows an implementation to define or use its own values and vocabularies.

4.1.3. Granularity. This represents the scope or limitation of the signal's applicability in terms of actors or context. Both GPC and ADPC do not explicitly define actors in their communication, nor provide the ability to specify the agents involved in the signal communication. Thus, both can have a 'global' scope, i.e., they can be expressed uniformly, e.g. at a browser level for all websites where the signal is set and for all actors. Both can also support a 'local' scope, whereby they can be independently expressed in specific contexts or for specific websites. It is worth mentioning that since ADPC supports the communication of free texts, contexts and actors can be specified as a part of the text. However, this is not explicitly described in the current proposal.

4.1.4. Format and Values. The *values* in a signal are distinct pieces of information related to the interpretation of the signal's intended information. The *format* is the 'shape' or 'structure' in which values are represented. Both *values* and *formats* have an impact on the effort required to interpret the signal and on the 'complexity' of the information that can be communicated. Both serve to determine the suitable 'vocabulary' and 'interfaces' that must be provided to the user for decision-making, expression and management. GPC is a unary signal, i.e., its values are limited to a single state (SET), therefore their interpretation is straightforward. ADPC does not specify a strict structure, but is akin to the expression of a 'policy' consisting of fields related to consent and objection to legitimate interests. ADPC does not provide a vocabulary or a structure for the development of vocabularies about the values expressed in its fields.

4.2. Signal Interpretation

4.2.1. Interpretation of Absence. The *absence* of a signal refers to a situation where no signal is communicated and its implications. Neither GPC nor ADPC define the interpretation of their absence. While this is not a necessity, it is important to consider, since a lack of signal may influence what controllers interpret as a permission (opt-out) or prohibition (opt-in).

4.2.2. Feedback of Signal Expression. *Feedback* refers to the response sent by the recipient of the signal based on the signal's values. The feedback can be an acknowledgement of the communication of the signal itself, or specific to a contextual event, such as a change in the signal's state or values. Neither GPC nor ADPC define a mechanism for feedback. For clarity, we split this factor into *feedback of expression* and *on change* in the summary table.

4.3. Signal Communication

4.3.1. Medium of Expression. The *medium of expression* refers to the specific mechanism through which the signal's information is communicated from the sender to the recipient. GPC and ADPC convey values through HTTP headers or DOM elements, with ADPC also supporting communication through JavaScript.

4.3.2. Recipient and Sender. These entities are considered as factors to identify the disparity between who *provides* the ability to express the signal and set its values and who receives that value. For GPC, the signal is expressed by the user-agent and received by the controller (or whoever is operating the servers). Based on its design, ADPC features both users and controllers as recipients of the signal expressed by websites and user-agents respectively, as it allows policies to be communicated between the two.

4.3.3. Propagation of Signal. The signal must be shared with all the actors involved in data flows to accurately convey its intention. Neither GPC nor ADPC address how it should be propagated to other actors where the communication does not directly occur between the party and the user.

4.4. Contextual factors

4.4.1. Developer and Maintainer. The developer signifies the entities or communities that affect the development, interpretation, and deployment of the signal, and allows discovering the stakeholders involved. GPC and ADPC were developed through small closed initiatives. As described in Section 2, GPC's creation involved US-based browser vendors, publishers, companies in the privacy sector, and academics. ADPC's development involved academics and an NGO in the Austrian RESPECTeD research project.

4.4.2. Fingerprinting Risks. By providing additional surfaces for tracking and profiling, unique combination of signal values present a "fingerprinting risk". The more values a signal expresses, the greater the risk. GPC represents minor risks given its binary states (that is: SET, NOT PRESENT), whereas ADPC does not present restrictions on the values or vocabularies used and thereby leads to a large surface for fingerprinting.

4.4.3. Enforcement and Enforceability. This refers to the defined interpretation and enforcement of a signal's value *by design and by definition*, but differs from legal enforcement based on the interpretation of the actions, values, and context of a signal with respect to the fulfilment (or violation) of legal obligations in data protection legislation (such as the GDPR). Both GPC and ADPC refer to specific legal obligations in their specifications, with GPC being enforceable under the CCPA. Both GPC and ADPC express potential for application under the GDPR (consent provision and withdrawal, respectively in Recital 32, Article 4(11), Article 6(1)(a) and Article 7; right to object in Article 21) and the ePrivacy Directive.

4.4.4. Loopholes in Interpretation. This factor considers if there are known *loopholes* in the interpretation of the signal — that we define as any condition or event preventing the correct interpretation of a signal's values. An example is that none of the signals specify how conflicts with other values or signals should be addressed [14]. GPC and ADPC do not clarify how to interpret which signal takes precedence when conflicting interpretations are possible through differences between the signal's communication and the user's actions (e.g. a mismatch when a user expresses a permission through a consent dialogue while the signal communicates a prohibition).

4.4.5. Application of Signal. This represents the specific activity or action the signal aims to change or regulate.[14] Most of the existing signals relate to tracking, surveillance, and permission to share data in some way. GPC is meant to prohibit "selling" (as defined by CCPA) or sharing of personal data with "any party other than the one the person intends to interact with". ADPC serves to provide or withdraw consent and object to direct marketing or use of legitimate interests (regardless of who the user interacts with). This factor is split into three lines in the summary table for the sake of clarity.

4.4.6. Stability and Technical Standardization. The *stability* of a signal represents the potential for change in interpretation, implementation, or methods. GPC can be considered as being stable (as it is implemented by browsers and respected by some service providers), although it is not standardized yet (e.g. by W3C or other standardization organizations). ADPC is a proposed specification that currently lacks extensive adoption and — similar to GPC — is not yet technically standardized by standardization organizations.

4.4.7. Auditability. This relates to the possibility to investigate the expression of the signal's value and whether and how it is acknowledged and respected. GPC and ADPC are simple to investigate, as one only needs to capture and inspect the HTTP communications between user-agent and servers.

4.4.8. Adoptability. This factor concerns whether the signal can be adopted by stakeholders other than those that developed the signal and the use in different use-cases and domains. GPC and ADPC can be expressed by any user-agent or actor on any device or platform. To date, GPC has been adopted by some browsers (e.g., Firefox, Brave, DDG) and some website / service providers (e.g., DDG, NYT, etc.)

4.4.9. Agency. This refers to the actor on whose behalf the signal is acting. Although it can be argued that all privacy signals are based on the *agency of the user*, an alternative perspective considers who controls the signal and its expression. GPC and ADPC represent the agency of the user in communicating intent, while ADPC also represents the agency of the controller in making requests to the user.

5. Current Personal Data Protection and Consent challenges to DPCCMs

Based on the results of our expert study, the following challenges to DPCCMs (summarized in Table 2) were selected: i) human centricity and HCI, ii) accountability, auditability and transparency, iii) legal enforcement, and iv) technical implementations. [15]

5.1. Human-centric and HCI Challenges

A shift of both decision-making power and structure from data controllers to data subjects could position the data subjects in the centre of data protection mechanisms.

H-1: Imbalance of power. Currently, the data controller decides the purposes and means of data processing [16]. This leaves data subjects in a vulnerable position with an imbalance of power, where they cannot express their privacy preferences.

H-2: Respect User Constraints. The upsurge of the way in which current consent dialogues are designed reveals limitations related to human cognition, in particular information and choice overload and fatigue [8], [17]. Users are often deceived by tools that intend to support and offer cognitive, collective, contextual assistance–through which the human-centric practice of online consenting can be enabled [8], [9], [18].

14. It can also be referred to as the 'scope' of the signal's application–though this term can be confused with scope as in the boundaries of contexts to which the signal can be applied.

15. Other (ethical, socio-technical diversity, organizational, societal, economic) challenges were identified, but we only report the four categories that were ranked higher due to the page limit.

16. For example, data subjects have little control over their consenting experience - which is mostly determined by the UI/UX of so called "consent banners" UI and underlying technologies

TABLE 1. TECHNICAL COMPARISON OF GPC AND ADPC BASED ON THE IDENTIFIED TECHNICAL FACTORS

Factor	*Description*	*GPC*	*ADPC*
	Signal contents		
Captured intent	What action is intended through the signal?	Opt-out	Opt-in/opt-out
Extensibility	Can the signal be expanded for additional use-cases/applications?	No	Yes
Granularity	How granular can the signal be expressed in terms of actors?	Unspecified	Unspecified
Format	What form is the signal expressed in?	Single Value	Policy
Values	What values can be sent?	Unary	Unbound Set
	Signal interpretation		
Interpretation of absence	What is the default interpretation when signal is not set (absence)?	Unspecified	Unspecified
Feedback of communication	Does the signal provide any feedback after expression?	No	No
Feedback on change	Is a change in the value of the signal acknowledged?	No	No
	Signal communication		
Medium of expression	How is the signal expressed i.e. mediums, formats?	HTTP, DOM	HTTP, DOM, JS
Recipient	Who receives the signal?	Website	Website, User-Agent
Sender	Who sends the signal?	User-Agent	Website, User-Agent
Propagation	Can the signal be propagated to multiple stakeholders?	Undefined	Undefined
	Informative		
Developer and maintainer	Who develops and maintains the signal?	GPC (group)	ADPC (group)
Fingerprinting risks	Does the signal expose surfaces to fingerprinting?	Minor	Major
Legal Enforcement	Is the signal legally enforceable?	CCPA, proposed for GDPR	Proposed for GDPR
Enforceability	Does the signal address specific legal clauses?	CCPA, GDPR, ePD	GDPR, ePD, ePR
Loopholes	Can known loopholes jeopardise the signal's interpretation?	Yes	Yes
Scope of application	What is the scope of impact or implementation of the signal?	Internet	Internet
Domain of application	Is the signal limited to specific domains or use-cases?	No	No
Purpose of application	Does the signal declare specific applications?	Selling data	General/Customizable
Stability	How stable is the signal's specification and interpretation?	Stable	Proposal
Technical Standardization	Is the signal [technically] standardized?	No	No
Auditability	Who can audit the signal?	All	All
Adoptability	Can the signal be adopted by other stakeholders?	Yes	Yes
Agency	On whose behalf does the signal act?	User	User/Controller

H-3: Display concise, comprehensible, but complete information. It has been shown that cookies and risks associated with them are generally poorly understood by web users [19]. Moreover, language in consent requests can be complex, incomplete, vague and misleading [20]. How to provide complete information about data processing practices, while being concise and direct, is an open question. In this regard, Kulyk et al. [21] found that users appreciated tools that helped them to better understand cookie browser settings with clear explanations about the purpose of data collection and the consequences of consent to their privacy. Later research by Elbert et al. [22] indicates how well-designed consent notices can improve understanding of privacy practices by highlighting important features.

H-4: Enforce Good Practices. Utz et al. showed that design patterns can be used to increase consent rates [23], a practice now known as "consent optimization". Service providers and consent managers make use of "dark patterns" to manipulate users into consenting [4]. When used to nudge users towards privacy-invasive settings and unduly steer consent decisions, manipulative designs have ethical and, in most cases, a legal import [2]. In this regard, the EU Parliament recently voted on the proposed Digital Services Act [17] to include a "ban on dark patterns" relating to consent and to offer options based on "tracking-free advertising" in case consent is refused or withdrawn to avoid coercion via tracking walls.

5.2. Accountability, Auditability and Transparency Challenges

Accountability refers to the property of a system that allows its inspection, monitoring and measurement from the outside. It can also be connected to transparency, user empowerment [24] and control over their personal data.

A-1: Accountability Artefacts and Repudiation. An ideal consenting system should be able to produce authentic artefacts, such as records of processing activities, that can support its inspection, both by watchdogs during an investigation and by the individuals themselves. Such artefacts must be sufficient, complete and available at any point in time. Note that a simple threat to any consent model is that a data controller can claim *plausible deniability* by claiming that either the signal was not received or that an external process manufactured it outside of the user's direct control. While it adds algorithmic complexity, accountability can be achieved at no cost to the user experience [25]. DPCCMs that only generate binary signals do not, on their own, meet sufficient accountability requirements. Accountability is best observed when confronted with a threat model, where the risks to privacy or compliance are identified and modelled [26]. The key limitation is the lack of interactivity and the notion of *session*, i.e., the fact that simple DPCCMs are unidirectional rather than based on long-lived user identifiers or stored states. This stems from the fact that accountability requires data authenticity which, in turn, relies on essential secure exchange/negotiation of data (e.g., to prove a claim

17. https://www.europarl.europa.eu/news/en/press-room/20220114IPR21017/digital-services-act-regulating-platforms-for-a-safer-online-space-for-users

such as "I Consent to the stated conditions") and, thus, requires bidirectionally. Two forms of authenticity exist: 1) direct/peer-to-peer negotiation or 2) engagement of a jointly trusted third party to notarise claims.

A-2: Post-Consent access to information and decisions. The expression of one's own privacy preferences is cumbersome, thus new interfacing mechanisms such as self-service privacy dashboards [27] are needed. Post-consent access is a further challenge, as users' preferences may change over time. Thus single actions should not be definite, irrevocable, and with long-lasting effects [28] and consent should not be modelled as a single point decision [29], [30].

A-3: Proof of Identity. Any signal needs to consider the consent life cycle, which entails that users can (or should be able to) modify their original decisions and exercise their rights, e.g., to erasure and of access. These actions require the ability to verify the identity associated with a request [31] to protect against attacks such as modification or illegitimate access.

5.3. Legal Challenges

Current legislation, such as the GDPR, the ePrivacy Directive, and the CCPA, provides the regulatory framework to which DPCCMs must abide. However, the practical implementation of the legal principles and rules often proves to be extremely challenging [32].

L-1: User preferences containing personal data. Whenever a DPCCM enables users to express their preferences, it might process personal data, such as a user's IP address [33] or another online unique identifier which requires compliance with data protection obligations, including the integrity and security of the signal (GDPR, Article 5(1)(f)), and an appropriate legal basis. In addition, DPCCMs might need user identifiers, such as IP addresses, to ensure continued application. When combined with unique personal identifiers and information from other sources, these online identifiers increase the risks of identifiability even when a user has not expressed her consent to any kind of personal data collection, triggering personal data breach (Articles 4(12), 5(1)(f), 32 GDPR). For example, a recent decision by the Belgian Data Protection Authority (APD) highlights some of the most pressing legal challenges that DPCCMs currently face. This decision [34] holds that the Interactive Advertising Bureau Europe's Transparency & Consent Framework (IAB TCF), a consent industry standard, failed to establish a legal basis for the processing of consent signal strings, and that the legal bases offered by the TCF were inadequate.

L-2: Legal requirements. Under the CCPA, users are entitled to concrete substantive rights, as follows. 1) The right to opt-out of sale: websites are required to provide "*a clear and conspicuous link*" on the homepage of their website entitled "Do Not Sell My Personal Information" or "Don't Sell My Personal Info" that allows users to invoke their right to opt-out of sale of their personal information (sections 1798.120, 1798.135). 2) The right to receive information, upon request, on the categories of personal information to be collected and right to be informed of the purposes for which such data shall be used. This information should enable a "meaningful understanding" (section 1798.100). 3) The right to delete personal information about the consumer that a website has collected (section 1798.105). Article 5(3) of the ePrivacy Directive and Articles 4(11) and 7 of the GDPR require that consent is freely given, prior, informed, specific, unambiguous, readable, accessible, and revocable. Moreover, the GDPR requires any consent management platform, acting as a data controller, to offer transparent information to users, as listed in Articles 13 and 14 (purposes, recipients, rights, storage, legal basis, etc.) to enable users to adequately consider the options before taking a decision. However, neither the GDPR -nor the EDPB in its guidance- provide methods or means to verify compliance: it does not indicate the procedures to guide the operationalization or enforcement of its principles, nor provides guidelines to perform systematic audits. Due to the large amount of information involved, compliance with these requirements is very complex from a technical (and HCI) perspective.

L-3: Information overload. Users can't realistically read all the privacy notices of the online services they interact with. Bravo-Lillo et al. [35] call this phenomenon "pop-up fatigue" or "habituation" to describe the tendency to ignore relevant information in circumstances where users are repeatedly confronted with it, such as consent dialogues and privacy policies. Thus, the strict implementation of the above regulations is almost futile if consent dialogues are doomed to be ignored. This questions whether the implementation of the current consent and information requirements is legally valid [36].

L-4: Standardization. Past experiences showed that working with non-interoperable and misaligned requirements and signals [37] may undermine the very purpose of such protocols to effectively communicate the data processing preferences and decisions of users. Thus, standardisation offers guarantees that bad faith website providers cannot hide behind non-interoperability claims to reject Internet users' signals [38]. Nevertheless, there is a multiplicity of competing standardisation endeavours – what has been commonly called as a 'jungle of standards' [39] in the field of data protection. A study conducted for the European Cybersecurity Agency, ENISA, showed there is a need for a structured approach on how privacy related standards are selected, agreed upon, and prioritised [40]. Currently, the selection of a suitable standard or specification lies mostly at the discretion of the website provider or vendor, since there is no legal or other obligation to conform to a specific DPCCMs. Moreover, the voluntary nature of technical standards and specifications [41] leads to a *lack of vertical enforceability* thereof. While in the US for example, standards of the National Institute of Standards and Technology (NIST) are mandatory for federal agencies and their contractors, technical standards and specifications in the EU are, in principle, not mandatory. As a result, even when a website provider undertakes to apply and conform to a certain DPCCM protocol, there is no direct administrative or other penalty for not respecting

the signal received in line with the Communication Protocol, if website providers demonstrate they comply in other ways with the applicable data protection law. Standardisation efforts are often the result of compromise of negotiations among entities participating in technical standardisation committees. "Political, economic, and social effects can be hard coded into protocol designs." [42]. The importance of ensuring good governance of standardisation bodies was also recently highlighted by the European Commission (2022) [43], which pointed at integrity, inclusiveness and accessibility of European Standardisation Organisations. Especially the standardisation of DPCCM Protocols should respect those principles, considering the possible impact of those protocols on fundamental rights of the right to protection of personal data, and other freedoms, such as the freedom of expression and human dignity [44].

5.4. Technical challenges

Technological diversity raises numerous challenges, as the technical settings for data protection and consent management can be as diverse as the contexts in which data collection happens (e.g., on the Web or in physical environments such as the Internet of Things (IoT)). DPCCMs must therefore account for the diversity of different technological setups, as they can be difficult to implement in IoT environments due to the lack of appropriate interfaces of devices, their *passivity*, and their low computational power.

T-1: Technological variety. Domain and application-specific solutions might be helpful in the short term, but might soon fail to deal with the complexity of protecting humans' privacy and agency throughout the whole system of interconnected processes, while keeping the system well functioning and sustainable. For example, the IoT is made of various protocols and types of technologies, thus generic solutions need to be carefully devised in order to encompass such variety [45]. Even if the IoT is by far the more diverse environment, variety can also be found on the Web. For instance, the Web can be navigated through different browsers on different types of machines with different operating systems, impacting how DPCCMs can be implemented.

T-2: Specificities of environments. Existing DPCCMs on the web use JavaScript or HTTP, but the IoT technological stack is quite different. For example, individuals are more prone to be physically tracked through their smartphones in the IoT [46], most of the time unbeknownst to them. Accordingly, consent management needs to be more adequately implemented using appropriate technological stacks in different environments [47], [48]. In addition, IoT devices are often devoid of proper interfaces to convey information, which in the worst-case results in individuals being tracked without being aware of it. Moreover, some devices are unable to actively communicate due to their limited computational power. These limitations must be taken into account when designing DPCCMs, otherwise large parts of the technological landscape will be unable to account for privacy signals.

T-3: Contents of information. The DPCCM's contents refer to the 'language' used to communicate a decision. While this typically includes interpretation of a particular value or symbol, it also includes defining interpretation when a value is missing or not conveyed. The content of the information communicated reflects the expressiveness of DPCCMs. While simple DPCCMs are easy to parse and understand, and therefore tend to have homogeneous interpretations and applications, complex DPCCMS are comparatively more difficult to utilise, although they offer richer information to convey.

T-4: Communication of information. A DPCCM should express and communicate information related to the preferences, decisions, or policies between service providers and users. Simple signals can be expressed using minimal data and can thus be transmitted frequently, whereas complex information requires either 1) a summarised or alternative representation or 2) an alternative model where it is expressed selectively (e.g. on first visit). An important part of the communication is the acknowledgement of the decision, both from data subjects and from controllers. When a DPCCM communicates an intention or a decision, the capability of the same signal or protocol to receive acknowledgement from the other party or agent is important to understand whether: (i) it supports the DPCCM; (ii) it has understood and acknowledged the decision; and (iii) there is any further relevant communication.

6. Comparison and Discussion

The primary value of both GPC and ADPC specifications is that they provide a substitute for communication of end-user decisions besides — or as a replacement of — current consent mechanisms (e.g. consent dialogues). However, both proposals do not address Section 5's challenges in the same way.

Human-centric challenges: Both GPC and ADPC can contribute towards a shift from an imbalance of power to user-centric practices (**H-1**), but in different contexts, ways and levels (see Section 4 for technical details). Because GPC's validity under the GDPR is still an unclear matter, a signal with a single application or value might be applicable only to specific domains and conditions and do not satisfy the requirement to communicate other user preferences and decisions (**L-2**). Therefore, websites would still have the necessity to use *consent dialogues*, thus leaving the existing human-centric challenges unresolved (see **H-2**, **H-3**, **H-4**).

ADPC features the communication of the processing purpose, along with a textual human-readable description that can be used to provide relevant information, typically provided through *consent dialogues*, such as that required by GDPR's Article 13. This information can then be used to generate and present dialogues to the users by their user-agents (e.g. browsers). If ADPC is made legally mandatory for websites to implement and support, and hence, for websites to not show consent dialogues, it would need: i) an implementation on user-side with sufficient information and ability for the

TABLE 2. MAIN CHALLENGES OF DPCCMS

Challenges
Human-centric and Human Computer Interaction
H-1: Imbalance of power
H-2: Respect of User Constraints
H-3 : Display concise, comprehensible, but complete information
H-4: Enforce Good Practices
Accountability, Auditability and Transparency
A-1: Accountability Artefacts and Repudiation
A-2: Post-Consent access to information and decisions
A-3: Proof of Identity
Legal
L-1: Users preferences containing personal data
L-2: Legal requirements
L-3: Information overload
L-4: Standardization
Technical
T-1: Technological variety
T-2: Specificities of environments
T-3: Contents of information
T-4: Communication of information

user to understand and make decisions; ii) similarity between the purposes and decisions communicated by ADPC and the ones that are shown in a consent dialogue; or iii) the website's integration of the ADPC's expressed preferences and decisions in its consent dialogue to offer users a meaningful option. Without such legally mandated requirements, ADPC would need proactive willingness from websites to be supported and effective in resolving known issues — which has been historically shown to be unrealistic (see the case of DNT). GPC can fulfil **H-2** more easily due to its unary signal, since it only communicates a single value — which requires a simple interface capable of binary states (e.g. set/unset checkbox). If ADPC is similarly used as a single-value fixed-vocabulary signal, it can be expressed by users using simpler interfaces (e.g. checkboxes or dropdowns). However, if ADPC does not utilise a fixed or controlled vocabulary and each website can potentially include new information communicated through ADPC, then this necessitates the use of additional mechanisms by which the website and user agree on what the communicated information implies (see **H-2**). This can be achieved by resorting to a controlled or standardised vocabulary with agreed-upon semantics and interpretations (e.g. the controlled vocabulary for purposes in TCF or the semantically matched concepts in the Data Privacy Vocabulary (DPV) [49]). Since GPC does not support communicating additional information, **H-3** and **H-4** are not directly relevant to its implementation. However, these challenges are important for ADPC where a large vocabulary is used, requiring additional tools and interfaces to allow the user to express a decision *dynamically* or *contextually*. These tools could be part of existing interfaces generated by user-agents (e.g. browsers), such as dialogues requesting permissions or dashboards for management, representation, and visualization of preferences and decisions i.e. **H-2**, **H-3**, and **H-4**.

Accountability challenges: None of the specifications expect a confirmation such as an acknowledgement from the data controller, i.e., an accountability artifact (**A-1**). However, user-agents can keep a copy of the decisions sent. For the GPC unary signal, this information consists only of its expression to a website. For ADPC, a record of the received requests and decisions made by users can be stored to change or withdraw consent and objections — thereby addressing challenges **A-2** and **A-3**.

Legal challenges. The legal enforcement to which each signal refers to will directly impact the requirements (**L-2**) and communication of consent-related information (**L-3**) for the selected specifications, since both the GPC and ADPC propose application under the GDPR, with GPC being only enforceable under CCPA. **L-2** and **L-3** are relevant for both signals, as information is required to be provided to users besides the existence of that signal's application. ADPC requires providing users with granular information and support [9] to fulfil both human-centric (**H-2**, **H-3**, **H-4**) and legal (**L-2**, **L-3**) requirements. **L-1** remains a challenge for both signals. Regarding **L-4**, a thorough study is necessary to explore how both standardization efforts correspond to good governance principles required by the EU regulations. Venues to identify complementarity of initiatives, such as the one studied in this paper, might be a necessary step to combat the proliferation of standards and specifications. The current ePrivacy Regulation proposal – facing trialogue negotiations, is yet to define relevant aspects of automated privacy signals. For example, whether browsers, and other software placed on the market permitting electronic communications (such as automatic privacy signals) will be set to prevent tracking individuals' digital footsteps by default.

Technical challenges. T-1 and **T-2** are both yet unsolved challenges for GPC and ADPC: both are communicated through HTTP headers and DOM elements, with ADPC additionally supporting programmatic invocation through JavaScript. Neither is inherently capable of supporting alternate environments (e.g. IoT, smartphones). This indicates the need for further developing extensions or additional protocols for their expression. **T-3** is not applicable for GPC, since it uses only a single-value communication of users' preferences. ADPC only specifies a structure for how information should be communicated, but requires additional vocabularies that must be supported by both websites and user(-agents) so as to agree on the contents and interpretation of information. As for **T-4**, a website operating under CCPA must support GPC as a legally-enforceable signal. Outside of this jurisdiction, however, both GPC and ADPC face challenges in fulfilling the three acknowledgment requirements regarding **T-4** in terms of whether they support the

signal, acknowledge its communication, and provide feedback in return.

7. Conclusion

In this paper we compared two current *open specification* DPCCM proposals, i.e the Global Privacy Control (GPC) and the Advanced Data Protection Control (ADPC), according to the identified technical factors and some interdisciplinary challenges. We argued that tackling those requires further research and development to support the implementation of DPCCMs. More specifically, this paper identified critical requirements in terms of human-centricity, accountability, lawfulness, and technicality of a signal and its implementation, thereby providing a framework through which future developments can be analysed and discussed.

Acknowledgments

This paper has been partially funded by the Internet Foundation Austria (IPA) within the *netidee* call (RESPECTeD-IoT Grant#5937). Cristiana Santos is funded by RENFORCE. Harshvardhan J. Pandit has been funded by the Irish Research Council Government of Ireland Postdoctoral Fellowship Grant#GOIPD/2020/790. The ADAPT SFI Centre for Digital Media Technology is funded by Science Foundation Ireland through the SFI Research Centres Programme and is co-funded under the European Regional Development Fund (ERDF) through Grant#13/RC/2106_P2. For the purpose of Open Access the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission. Arianna Rossi and Wilhelmina Maria Botees have been partially supported by the Luxembourg National Research Fund (FNR) – IS/14717072 "Deceptive Patterns Online (Decepticon)".

References

[1] H. Smith, T. Dinev, and H. Xu, "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, vol. 35, pp. 989–1015, Dec. 2011.

[2] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. New York, NY, USA: Association for Computing Machinery, May 2021, pp. 1–18.

[3] A. Mathur, G. Acar, M. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites," *Proc. ACM Hum.-Comput. Interact.*, vol. 1, no. CSCW, 2019.

[4] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence," *arXiv:2001.02479 [cs]*, Jan. 2020, arXiv: 2001.02479.

[5] C. Wylie, *Mindf* ck: Cambridge Analytica and the plot to break America*. Random House, 2019.

[6] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 1st ed. New York: PublicAffairs, Jan. 2019.

[7] S. Human, "THE HALE WHALE: A Framework for the Co-creation of Sustainable, Human-centric, Accountable, Lawful, and Ethical Digital Sociotechnical Systems," *Sustainable Computing Paper Series*, no. 2022/01, 2022.

[8] S. Human and F. Cech, "A Human-Centric Perspective on Digital Consenting: The Case of GAFAM," in *Human Centred Intelligent Systems*, ser. Smart Innovation, Systems and Technologies, A. Zimmermann, R. J. Howlett, and L. C. Jain, Eds. Singapore: Springer, 2021, pp. 139–159.

[9] S. Human, R. Alt, H. Habibnia, and G. Neumann, "Human-centric Personal Data Protection and Consenting Assistant Systems: Towards a Sustainable Digital Economy," in *Proceedings of the 55th Hawaii International Conference on System Sciences*. Hawaii, USA: University of Hawaii, 2022, pp. 4727–4736.

[10] S. Human and M. Kazzazi, "Contextuality and intersectionality of e-consent: A human-centric reflection on digital consenting in the emerging genetic data markets," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2021, pp. 307–311.

[11] S. Zimmeck and K. Alicki, "Standardizing and implementing do not sell," in *Proceedings of the 19th Workshop on Privacy in the Electronic Society*, 2020, pp. 15–20.

[12] S. Human, M. Schrems, A. Toner, Gerben, and B. Wagner, "Advanced Data Protection Control (ADPC)," Vienna University of Economics and Business (WU Wien), Vienna, Sustainable Computing Reports and Specifications 2021/01, 2021.

[13] S. Human, "Advanced data protection control (adpc): An interdisciplinary overview," *Sustainable Computing Paper Series*, no. 2022/01, 2022.

[14] M. Hils, D. W. Woods, and R. Böhme, "Privacy preference signals: Past, present and future," *Proceedings on Privacy Enhancing Technologies*, vol. 2021, no. 4, pp. 249–269, 2021.

[15] "Decision on the merits 21/2022 of 2 february 2022? complaint relating to transparency & consent framework," 2022.

[16] K. Charmaz, *Constructing grounded theory*. sage, 2014.

[17] M. Burgess, "The tyranny of GDPR popups and the websites failing to adapt," vol. 22, p. 2019, 2018.

[18] S. Human, G. Neumann, and M. F. Peschl, "[How] can pluralist approaches to computational cognitive modeling of human needs and values save our democracies?" *Intellectica*, vol. 70, pp. 165–180, 2019.

[19] V. Ha, K. Inkpen, F. Al Shaar, and L. Hdeib, "An examination of user perception and misconception of internet cookies," in *CHI'06 Extended Abstracts on Human Factors in Computing Systems*, 2006, pp. 833–838.

[20] 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 *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. ACM, 2021, p. 187–194.

[21] O. Kulyk, A. Hilt, N. Gerber, and M. Volkamer, ""This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer," in *Proceedings 3rd European Workshop on Usable Security*. Internet Society, 2018.

[22] N. Ebert, K. Alexander Ackermann, and B. Scheppler, "Bolder is better: Raising user awareness through salient and concise privacy notices," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–12.

[23] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed Consent: Studying GDPR Consent Notices in the Field," in *Proc. CCS*, ser. CCS '19. New York, NY, USA: ACM, 2019, pp. 973–990.

[24] S. Human, R. Gsenger, and G. Neumann, "End-user empowerment: An interdisciplinary perspective," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, Hawaii, United States, 2020, pp. 4102–4111.

[25] V. Jesus and H. J. Pandit, "Consent receipts for a usable and auditable web of personal data," *IEEE Access*, pp. 1–1, 2022.

[26] V. Jesus, "Towards an accountable web of personal information: The web-of-receipts," *IEEE Access*, vol. 8, pp. 25 383–25 394, 2020.

[27] C. Bier, K. Kühne, and J. Beyerer, "Privacyinsight: The next generation privacy dashboard," in *Privacy Technologies and Policy*, S. Schiffner, J. Serna, D. Ikonomou, and K. Rannenberg, Eds. Cham: Springer International Publishing, 2016, pp. 135–152.

[28] V. Jesus, "Pragmatic online privacy: the sfte approach," in *1st Intl Workshop on Consent Management in Online Services, Networks and Things, with 6th IEEE EuroS&P*, 2021.

[29] A. Acquisti, I. Adjerid, and L. Brandimarte, "Gone in 15 seconds: The limits of privacy transparency and control," *IEEE Security Privacy*, vol. 11, no. 4, pp. 72–74, 2013.

[30] A. Adams. (2021-11-11) Algorithmic Decisions and Their Human Consequences — The Regulatory Review.

[31] C. Boniface, I. Fouad, N. Bielova, C. Lauradoux, and C. Santos, "Security analysis of subject access request procedures," in *Annual Privacy Forum*. Springer, 2019, pp. 182–209.

[32] C. Santos, N. Bielova, and C. Matte, "Are cookie banners indeed compliant with the law? : Deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners," *Technology and Regulation*, vol. 2020, p. 91â€"135, Dec. 2020.

[33] C. Santos, M. Nouwens, M. Tóth, N. Bielova, and V. Roca, "Consent management platforms under the gdpr: processors and/or controllers?" in *APF*, 2021.

[34] A. de protection des données, "Decision on the merits 21/2022 of 2 february 2022. case number: Dos-2019-01377. complaint relating to transparency & consent framework." 2022.

[35] C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, and M. Sleeper, "Harder to ignore? revisiting {Pop-Up} fatigue and approaches to prevent it," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 105–111.

[36] D. Lindegren, F. Karegar, B. Kane, and J. S. Pettersson, "An evaluation of three designs to engage users when providing their consent on smartphones," *Behaviour & Information Technology*, vol. 40, no. 4, pp. 398–414, 2021.

[37] W. Melicher, M. Sharif, J. Tan, L. Bauer, M. Christodorescu, and P. G. Leon, "(do not) track me sometimes: Users' contextual preferences for web tracking," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 2, pp. 135–154, 2015.

[38] I. Kamara and E. Kosta, "Do Not Track initiatives: regaining the lost user control," *International Data Privacy Law*, vol. 6, no. 4, pp. 276–290, 10 2016.

[39] N. C. Gleeson and I. Walden, "'it's a jungle out there'?: Cloud computing, standards and the law," *Eur. J. Law Technol.*, vol. 5, 2014.

[40] J.-P. Quemard, J. Schallabok, I. Kamara, and M. Pocs, "Guidance and gap analysis for european standardisation: Privacy standards in the information security context," 2019.

[41] A. Harcourt, G. Christou, and S. Simpson, *Global Standard Setting in Internet Governance*. Oxford: Oxford University Press, January 2020.

[42] Kiernan and Mueller, "Standardizing security: Surveillance, human rights, and the battle over tls 1.3," *Journal of Information Policy*, vol. 11, p. 1, 2021.

[43] "An eu strategy on standardisation. setting global standards in support of a resilient, green and digital eu single market, communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions com(2022) 31 final.)," 2022.

[44] P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. opacity of the individual and transparency of power," *Privacy and the criminal law*, pp. 61–104, 2006.

[45] V. Morel, M. Cunche, and D. Le Métayer, "A generic information and consent framework for the iot," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2019, pp. 366–373.

[46] L. Demir, M. Cunche, and C. Lauradoux, "Analysing the privacy policies of Wi-Fi trackers." ACM Press, 2014, pp. 39–44.

[47] M. Cunche, D. L. Métayer, and V. Morel, "Colot: a consent and information assistant for the iot," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 334–336.

[48] S. Giordano, V. Morel, M. O. Nen, M. Musolesi, D. Andreoletti, F. Cardoso, A. Ferrari, L. Luceri, C. Castelluccia, D. L. M. Tayer, C. V. Rompay, and B. Baron, "UPRISE-IoT: User-centric Privacy & Security in the IoT," in *SPIoT*, 2019, p. 17.

[49] H. J. Pandit, A. Polleres, B. Bos, R. Brennan, B. Bruegger, F. J. Ekaputra, J. D. Fernández, R. G. Hamed, M. Lizar, E. Schlehahn, S. Steyskal, and R. Wenning, "Creating A Vocabulary for Data Privacy," in *The 18th International Conference on Ontologies, DataBases, and Applications of Semantics (ODBASE2019)*, Rhodes, Greece, 2019, p. 17.