User-side Consent Dialogues and Management Using ADPC and DPV*

Harshvardhan J. Pandit

ADAPT Centre, Trinity College Dublin, Ireland me@harshp.com

Abstract. DRAFT FOR DISCUSSION ONLY CC-BY-NC-ND 4.0

Keywords: consent

1 Introduction

1.1 Motivation

The mechanisms surrounding consenting on the web are today rife with problematic issues (for an overview, refer to Section 2 that threaten its use as a means for people to exercise their agency and rights regarding privacy and data protection. The requirements established by the General Data Protection Regulation (GDPR) provide a legal framework through which authorities can take action against these issues and dissuade their prevalence. However, in practice, such enforcement has not been effective in terms of mitigating such issues despite the requirements of GDPR being known for 5 years (2016-2022). This has resulted in concerns regarding the performance and effectiveness of Data Protection Authorities (DPAs), and has resulted into an official enquiry by the EU Ombudsman[1] to look into the EU Commission's handling of GDPR enforcement. At the same time, DPAs have (repeatedly) indicated the lack of available expertise and funding required to be effective in their duties [].

To date, typical actions undertaken by DPAs have included specific investigations into problematic areas of technologies, such as facial recognition, and to issue guidelines that call upon organisations to effectively ensure their own compliance in the hopes of self-regulation fixing existing known problems. The few high-profile decisive cases, such as CNIL's fine to Google and Facebook regarding their consenting practices has failed to have a domino effect in terms of reactive changes in practices. GDPR allows for easing some of the investigation and compliance efforts through creation of codes of conduct and certifications. However, to date, no such mechanism exists that applies itself to remedy or prevent issues regarding consent. While IAB Europe has applied to utilise its Transparency & Control Framework (TCF) framework as a code of conduct [2], the recent decision by the Belgian DPA concerning the legality of TCF [**?**] and its

* Supported by organization x.

[1] https://www.ombudsman.europa.eu/en/opening-summary/en/149949

[2]

use by the advertisement industry raises important issues about its effectiveness if adopted. It also raises the question on how individuals and society at large do not have a medium to participate in such processes to outlay a balance between rights and requirements.

While all the above should be used in demanding greater effectiveness of the law through its enforcement agents (courts and DPAs), this article argues that such effectiveness should not rely solely on the capabilities of the organisations to self-regulate, but should instead motivate socio-technical solutions that mitigate the root causes of known prolonged issues. This would require a change within the EU's approach towards development and utilisation standards in connection with legal compliance, where the onus is always on assisting organisations with their legal compliance tasks. While the EU has promoted standards developments in a more globally cohesive manner, such as through co-operation agreement between CEN/CENELEC and ISO[3], it has refused to take any measures on the technologies and standards that underline the use of internet or its standardisation processes (e.g. IETF, W3C). As a result, the capabilities, values, and features developed within such technologies do not assist in any of the additional provisions and requirements established by the GDPR to increase the expected level of privacy and data protection.

For example, consider the prevalence of cookie banners to fulfil requirements of the ePrivacy Directive (2002) to provide information and management of cookies to users, and which are known to have widespread issues [], . In the 10 years of their existence, the underlying technological mechanisms in terms of how cookies can be set by websites and managed by users within their browsers have not changed in significance other than browsers attempting to prevent their usage in tracking and surveillance. To date, there is no cookie categorisation specification through which websites can clearly indicate what the cookies are necessary for, nor are there any cookie management interfaces for users within the web browsers. Now with GDPR, cookie banners have been supplemented with consenting interfaces that also show similar issues [], and demonstrate the same pattern of no fundamental developments being undertaken to remedy them at a technological level. To sum all of the above, this article raises the question, "*What significant developments are needed to ease the widespread application and use of consenting interfaces?*"

1.2 Existing Approaches

Researchers have proposed several interesting approaches regarding how users can express, communicate, manage, control, and enforce their privacy and decisions. However, this article focuses on concrete proposals used or proposed by stakeholder organisations as so limit the discussion to practicality and application in real-world issues. The focus here is on user-side solutions as alternatives to the industry-specified standards, such as the TCF and its exclusive use by

[3] https://www.cencenelec.eu/about-cen/cen-and-iso-cooperation/

Consent Management Platforms (CMPs), which can be argued to be cause of issues itself [**?**].

Existing standardised approaches such as Do Not Track (DNT) and Platform for Privacy Preferences (P3P) are either obsolete or abandoned, with new proposals including Global Privacy Control (GPC) and the Advanced Data Protection Control (ADPC) being candidates for investigation. GPC has been developed to be applied within California's Consumer Protection Act (CCPA), and is a unary (single value) signal that expresses 'do not sell' as per the CCPA's enforceable obligation of providing an option to prohibit organisations from 'selling' data to other third parties. GPC has been adopted by numerous high-profile websites such as the New York Times and is implemented by web browsers such as Brave and Firefox. ADPC is a specification for expression and communication of information regarding purposes and their use in giving or withdrawing consent and exercising the right to object. It was developed by None of Your Business (NOYB) as part of the RESPECTeD project., ADPC currently does not provide the necessary information for how such purposes should be expressed in an interoperable manner and the governance processes that should be followed by each actor i.e. websites, user-agents, and the users.

While both GPC and ADPC claim to be actionable under the GDPR and ePrivacy Directive as automated signals (e.g. GDPR Art.21-5), the difference in terminology in GPC[4] and the lack of details for implementation in ADPC bring this under question. The DPAs or other data protection bodies have also not commented on authoritative interpretations of these proposals.

1.3 Research Goals

Rather than expressing an entirely new proposal, this articles takes the view of that harmonised developments over existing proposals are better to consolidate stakeholder support. For this, it aims to resolve known issues and improve current consenting mechanisms by proposing novel use of existing information and communication protocols, namely HTML and ADPC respectively. Through these, proposes a radical alternative to the current status quo of website-controlled consent interfaces by demonstrating the implementation of user-side consenting interfaces is not only possible, but also useful, practical, and feasible. The rest of the article is structured in terms of the following research goals:

1. To analyse the extent to which existing issues regarding consent can be minimised or relegated by increasing user-controlled technologies
2. To demonstrate feasibility of implementations for ADPC regarding:
   (a) Communication of information regarding consent and decisions
   (b) Establishing a shared interoperable vocabulary
   (c) Generation of consent dialogues on user-side
   (d) Annotating consent dialogues and information with semantic markup
3. To critically evaluate the practicality of adopting proposed work through legal,industry,and socio-technical perspectives

[4] https://harshp.com/research/blog/gpc-gdpr-can-it-work

2 Categorisation of Issues from State of the Art

Table 1. Categorisation of issues related to 'consent' in SotA

GDPR Clause	HCI	IT	Law
freely given (R43)	nudging [15,2,5,7,8,11,12], consent wall [5,12,15,13], cannot refuse [9,12],preselected options [9,11,12], nagging [13]		tracking wall [16,4,11,12]
specific (R43)	wording [15,2,8]	cookie purposes [3], ignore preferences [9]	wording [11,10,9,12]
informed (R43)	framing [5,8,12,15,12,13], granularity [11,12], layering [11]	third party [2], cookie syncing [14], cookie purposes [3]	information required [12]
unambigious (R43)	[15,6,2], action or expression [12]	assume consent without action [9,12], assume given regardless of choice [9,12], transmission of signal [12]	
information provision (A13,A14)	broken links [6], missing information [6], excessive interactions [6], covertness [7]	cookie syncing [14]	
legal basis		incorrect for implementation [10]	unclear or incorrect [1,10], applicability of consent [10]
withdrawal (A7)	number of actions [11]	cookie [12], communication to third parties [12]	
explicit consent (A9)			consent should be explicit [1,2]

- Issues related to information: wording (description), framing (context), granularity (broad vs specific), missing information
- Issues related to presentation of information: wording, framing, granularity, layering, broken links, missing information, unclear or ambiguous information
- Issues related to presentation of choices/options: nudging, consent wall, disparity or imbalance between choices, preselected options, layering (hiding options)

- Issues related to expression of choice: no choice provided (e.g. no reject button), disparity in placement of choice (e.g. accept on 1st layer, refuse in 2nd), pre-selected options, granularity (e.g. agree all but refuse individually), layering (hiding choices in different layers), assumption (e.g. consent on scrolling or visiting), fatigue or no of actions (excessive actions e.g. to refuse all)
- Issues related to third-parties: hiding scale/scope of third party sharing, other issues applied for each third party (e.g. missing policies)
- Issues related to legal basis: incorrect legal basis (e.g. legitimate interest instead of consent), incorrect consent expression quality (e.g. not explicit)

3 Extending ADPC

1. Currently ADPC specifies multiple ways of obtaining information about the purposes: (1) Link in header to a file containing consent requests; (2) Script that calls the consent-request API and passes the information.
2. The websites determine which purpose terms they want to use. Simultaneously users (and user-agents) also need to be aware of the terms (and their variance) to enable expression of consent/object decisions. This creates too much information management overload if every website changes it terms or users have to manage it for every website individually.
3. There may be a hidden assumption that using a common specification, such as TCF, will reduce this issue, but this still leaves the ability for purposes to be a free-field text with no restrictions.
4. To rectify this, proposal is to walk through three steps of incrementally radical proposals: (1) Adopting existing specification i.e. TCF, which is fixed/final and cannot be modified or adapted; (2) Adopting existing specification i.e. DPV, which can act as a base vocabulary and provide adaptability; (3) Creating a standardised mechanism for registering purposes.
5. ADPC also does not define a way through which users can define broad preferences, e.g. object to all purposes of category X, which is necessary to reduce fatigue on user-side for managing all the different purposes and their constant variance across websites. Therefore the above three proposals should take into consideration the ability to create broad user-side preferences that can be compared and applied to incoming/outgoing signals.

3.1 Application to IAB's TCF v2

1. TCF string has a lot of additional info than just purposes
2. It contains information about which parties, which data, which legal basis, etc.
3. ADPC only defines purposes (loosely), though what else that term could be used for is not excluded from being interpreted i.e. the identifier '1A2B3C' can be the id of purpose 1A that uses data 2B for controller 3C. This approach enables is to adopt part of the TCF signal for purpose in consent requests.

4. Action is to create a mechanism by which part of the TCF string is converted to ADPC's specification of purposes.
5. The above needs to be defined in terms of whether that purpose/consent enables third-parties to obtain that data, as defined in TCF.
6. Action is to then compare user-side expression with controller-side requests. Whether broad ones can be defined e.g. do not accept any purpose that says XYZ or always object to ABC.
7. Communication of information through HTTP can be made efficient by utilising the binary form of TCF. This would (probably) result in at most 2-3 bytes if only the purposes and relevant information is used.

3.2 Establishing a shared vocabulary using DPV

1. DPV is a taxonomy of purposes, personal data, legal bases, etc. The taxonomy is structured top-down i.e. the top-most concepts in hierarchy are the most abstract, with more specific concepts below it. Most concepts will not be specific and accurate enough to be used as is for an use-case. The guidelines are to expand a concept to make it more specific e.g. Marketing (DPV) –¿ Marketing about new products (use-case)
2. To adapt the above for ADPC, requests contain two pieces of information, the purpose requested by the controller and the DPV concept it is expanded from. User-side can then utlise the known DPV category to assist the user in making decisions e.g. allow analytics as a purpose, deny tracking.
3. Action: DPV is a list of words, which are not great for use in HTTP. Similarly to ADPC, a binary expression can be created by converting DPV to a flat list and assigning identifiers (e.g. top concept is 0, next concept is 1, etc. (e.g. use Shannong-Fano encoding).
4. This taxonomy is richer than TCF, more flexible in that multiple purposes can be cleanly combined and retain individuality (i.e. multiple parent concepts), which is helpful for better user-side granular decisions
5. Users can easily make broader decisions e.g. saying all Marketing is okay would mean anything under Marketing concept is okay. Same for refusal/object.

3.3 Need for a Global Shared Registry

1. To avoid the constant declaration of which vocabulary is used, and to avoid/prevent a single restricted vocabulary such as TCF being the only applicable vocabulary, a globally acceptable standard registry needs to be established centrally e.g. W3C specification.
2. In this registry, pointers to finding the correct code are expressed in binary form similar to TCF usage. However, instead of directly pointing to a specific purpose, the code is broken into different parts that enable identifying which vocabulary to use.
3. For example, consider 4-byte words: 0110 1110 1010 0111 where the first bit (0) indicates this is a registered vocabulary and to look up the entry using the next seven bits (110 1110 = 108 of 127) identify the vocabulary

to use, and the next number of bits and their length are determined by the vocabulary used. In this case, vocab 127 says interpret the next 8 bits (or could be more or variable) as each bit indicating permission for a purpose in the list (same as TCF).
4. Creating such vocabularies and requiring some standardised expression is part of their governance process whereby authorities, public, etc. have the ability to specify additional information/requirements at the purpose level. For example, saying XYZ purpose in a list MUST require explicit consent, or that ABC MUST not be used with legitimate interest.
5. This is a weakly defined objective, but of interest in terms of standardisation, whether in W3C or ISO, as well as to expand the stakeholders present in the communication mechanisms and the utilisation of a signal.
6. Such a global registry is also very useful to have users express preferences in one vocabulary (e.g. DPV) and have the user-agent convert or map it to another vocabulary (TCF) based on the standardised entries within the registry.

4 Generating Dialogues on User-side

- Some of the current issues also relate to the UI / HCI side of dialogues for how information is presented, how options are presented, how consenting takes place (e.g. dark patterns). To rectify this, some or all of the consenting interface can be managed at the user-side by user-agent of choice (e.g. web browser or external provider)
- There are various options for doing this: controller only provides information (e.g. via ADPC) and receives a decision (true/false) with the interface being generated and interacted with on the user-side. Other options include controller being offered a framework within which they have to 'fit' or 'express' their information and choices where the framework is controller by the user-agent. Third option is to let the controller control all of the interface except the part where consenting actions are needed, which is handled by the user-agent.
- To distinguish between these elements, there needs to be some common acceptance on the terms for understanding each part. There is the notice which contains information. Notice elemnents are parts of a notice. Controls are actionable elements meant to be interacted with by the user (e.g. more info, select choice).
- Layering controls refer to information density, granularity, presentation, etc. Preference control refer to the user expressing a preference. It is important to note that a preference is not a final decision e.g. checkboxes. Decision controls are controls that convey the decision of the user e.g. accept/reject button.

4.1 Complete Generation

1. Controllers send information, user-agent creates interface, provides choices, and sends the decision back to the controller.

2. What information does this require e.g. GDPR A.13 / A.14. ADPC only conveys purpose and some text. Where will the rest of the information come from?
3. DPV can act to provide the complete information in machine-readable form i.e. the set Purpose, Processing, Personal Data, Controller, Recipients, Legal Basis, Tech/Org Measures
4. controllers can still customise the look and feel of individual elements e.g. using CSS

4.2 Providing Customisable Interfaces

1. Controllers retain the ability to customise interfaces i.e. using CSS, but have to use the provided framework to make requests
2. this means the user-agents provides something like createNotice() function that takes paraterms the contents of a notice (options for notice element, controls, styling, etc.)
3. Such an approach forces controllers to express notices and dialogues in granular form
4. It also enables user-agents to rectify or correct known issues such as disparity in consenting choices

4.3 Only Generating Choices and Expression

1. Controllers retain complete control of what they want to show and how; user-agent provides ability to specify the interface but requesting consent is still done through the user-agent provided API call
2. This could be something like requestConsent(html_element_id) where the HTML element ID refers to the ID of element containing the notice and choices elements, and whose return value would be a dictionary expressing the decisions made by the user
3. While this provides controller the abiliy to control how they want to make a request (and use dark patterns) the final decision making capability is specifed by the user
4. A more granular iteration of this option is the requirement to also require choices (e.g. checkboxes) also to be requested via the user-agent interface in addition to the final decision

5 Enriching Consent Interfaces with Semantic Markup

This has concrete proposals and implementations: see https://doi.org/10.5281/zenodo.5076603

The gist is that by embedding this information alongside the HTML elements, the user-agent can identify the notice elements and assist in the requesting and decision making process. This can be the source of information required for some of the proposed approaches above with the HTML existing as a fallback in case the user-agent does not support ADPC.

5.1 HTML elements

1. notice using the dialog HTML element
2. customising buttons/choices
3. indicating action/application/information using data-* attributes

5.2 Semantic Annotations

1. schema.org , despite aiming to offer rich semantic markup for websites, has absolutely no concepts to represent things such as privacy policies, t&c, entities and roles (e.g. controller), dialogues and interfaces, consent, preferences, etc.
2. Proposal to add these concepts to schema.org so they can be used in HTML to identify notice elements and its contents e.g. to indicate which button is consent action
3. Some of these concepts could be deemed to not be in scope for schema.org, therefore they could be expressed with either DPV (where concepts exist) or necessitate the creation of another vocabulary

6 Discussion on Practicality and Feasibility in Real-World

- Why would controllers use this
- Why would user-agents develop this
- Why would users want to choose/use this
- Why would DPAs / NGOs like this
- Where would their legal enforceability come from
- What needs to be done in law for their development
- Who develops these standards? If left to only partial industry e.g. ad-tech or american companies, the history has been no significant developments to address this.

7 Conclusion

References

1. Costello, R.Á.: The Impacts of AdTech on Privacy Rights and the Rule of Law. Technology and Regulation pp. 11–23 (Apr 2020)
2. De, S.J., Imine, A.: Consent for targeted advertising: The case of Facebook. AI & SOCIETY (May 2020). https://doi.org/10/ggzp38
3. Fouad, I., Santos, C., Kassar, F.A., Bielova, N., Calzavara, S.: On Compliance of Cookie Purposes with the Purpose Specification Principle. In: IWPE. p. 9 (2020)
4. Gil González, E., de Hert, P.: Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. ERA Forum **19**(4), 597–621 (Apr 2019). https://doi.org/10/gf6mnt

5. Gray, C.M., Santos, C., Bielova, N., Toth, M., Clifford, D.: Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. arXiv:2009.10194 [cs] (Sep 2020)
6. Habib, H., Zou, Y., Jannu, A., Sridhar, N., Swoopes, C., Acquisti, A., Cranor, L.F., Sadeh, N., Schaub, F.: An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. In: Proceedings of the Fifteenth Symposium on Usable Privacy and Security. p. 21. Santa Clara, CA, USA (Aug 2019)
7. Human, S., Cech, F.: A Human-centric Perspective on Digital Consenting: The Case of GAFAM. In: Human Centred Intelligent Systems 2020. Split, Croatia (2020)
8. Machuletz, D., Böhme, R.: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. Proceedings on Privacy Enhancing Technologies **2020**(2), 481–498 (Apr 2020). https://doi.org/10/ghqdq8
9. Matte, C., Bielova, N., Santos, C.: Do Cookie Banners Respect my Choice? In: 41st IEEE Symposium on Security and Privacy. p. 19 (2020)
10. Matte, C., Santos, C., Bielova, N.: Purposes in IAB Europe's TCF: Which legal basis and how are they used by advertisers? In: Annual Privacy Forum (APF 2020) (Oct 2020)
11. Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems pp. 1–13 (Apr 2020). https://doi.org/10/ggx9vq
12. Santos, C., Bielova, N., Matte, C.: Are cookie banners indeed compliant with the law? deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Technology and Regulation pp. 91–135 (Dec 2020). https://doi.org/10/ghtr3n
13. Soe, T.H., Nordberg, O.E., Guribye, F., Slavkovik, M.: Circumvention by design – dark patterns in cookie consents for online news outlets. arXiv:2006.13985 [cs] (Jun 2020)
14. Urban, T., Tatang, D., Degeling, M., Holz, T., Pohlmann, N.: The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR. arXiv:1811.08660 [cs] (Nov 2018)
15. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: ACM SIGSAC Conference on Computer and Communications Security (CCS'19). p. 18. London, United Kingdom (Nov 2019)
16. Zuiderveen Borgesius, F.J., Kruikemeier, S., Boerman, S.C., Helberger, N.: Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. European Data Protection Law Review (EDPL) **3**(3), 353–368 (2017). https://doi.org/10/gfsh4x