



Engaging Content  
Engaging People



Trinity College Dublin  
Coláiste na Tríonóide, Baile Átha Cliath  
The University of Dublin



IRISH RESEARCH COUNCIL  
An Chomhairle um Thaighde in Éirinn



# Consent: Where are we going?

Harshvardhan J. Pandit

Postdoctoral Fellow

ADAPT Centre, Trinity College Dublin

<https://harshp.com/research>

[pandith@tcd.ie](mailto:pandith@tcd.ie)

MDPP DCU, Monday MAR-15 2021



European Union  
European Regional  
Development Fund



Research Fellow @ Trinity College Dublin

Currently working on: Semantics x Privacy Risks x GDPR x Consent

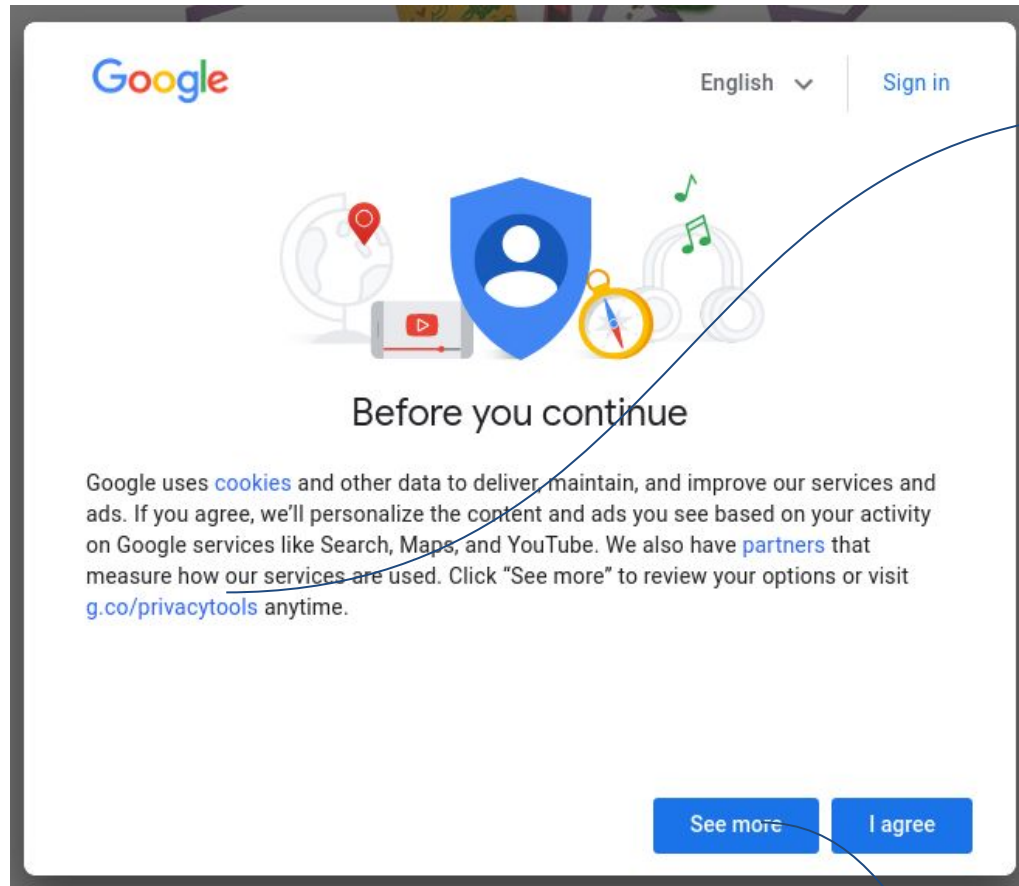
PhD: 2016-2020 Computer Science, Trinity College Dublin

Representing Activities associated with Processing of Personal Data and Consent using Semantic Web for GDPR Compliance

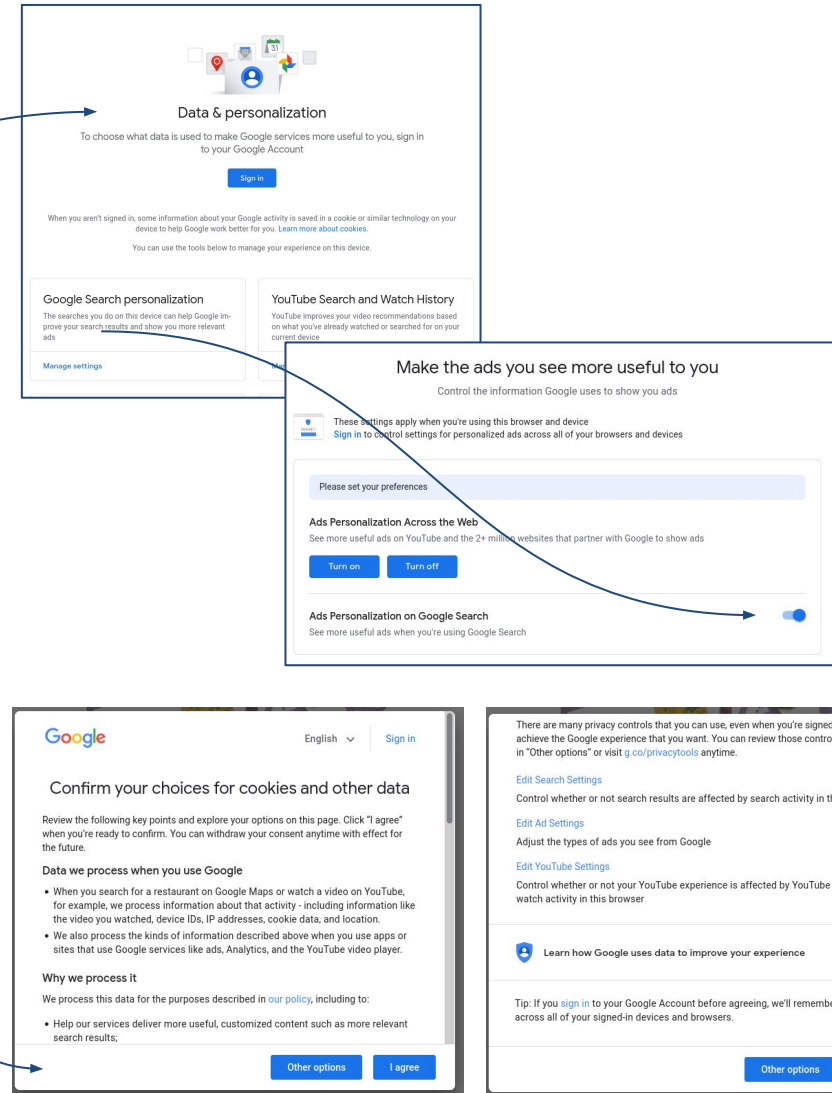


# “consent” is not an optional choice

slide#3



Consent dialogue on <https://google.ie> MAR-14 2021



[www.adaptcentre.ie](http://www.adaptcentre.ie)

Consent should be:

1. Freely given → without coercion, no obligation
2. Specific → exact and limited in scope
3. Informed → prior knowledge of consent and consequences
4. Un-ambiguous → clear indication of consenting
5. Revocable / Can be Withdrawn → once given, can be cancelled

- GDPR Art. 4-11 (2016)

The image shows a screenshot of a Quantcast privacy consent banner. The banner is white with a red border. At the top, the word "identity" is written in red. Below it, the Quantcast logo is displayed with "Quantcast" in black and "identity" in red. The main heading "We value your privacy" is in black. Below this, the text "purpose" is written in red. The body text explains that Quantcast and its partners use cookies to personalise content and ads, provide social media features, and analyse traffic. It also states that users can change their consent choices at any time. Below the text, there are two buttons: "I DO NOT ACCEPT" and "I ACCEPT". The word "revocation" is written in red above the buttons. At the bottom, the text "Indication of consent" is written in red, with "Show Purposes" in smaller text below it. The banner is powered by Quantcast.

identity

**Quantcast**

We value your privacy

purpose

We and our partners use technology such as cookies on our site to personalise content and ads, provide social media features, and analyse our traffic. Click below to consent to the use of this technology across the web. You can change your mind and change your consent choices at anytime by returning to this site.

revocation

I DO NOT ACCEPT I ACCEPT

Indication of consent

Show Purposes

Powered by Quantcast

GDPR Art 4, 7, 13, 14

Identity of Controller

Purpose

Processing Categories

Personal Data Categories

Right to Withdraw Consent

Data Storage Periods

Data Sharing / Recipients

Trans-border data flows

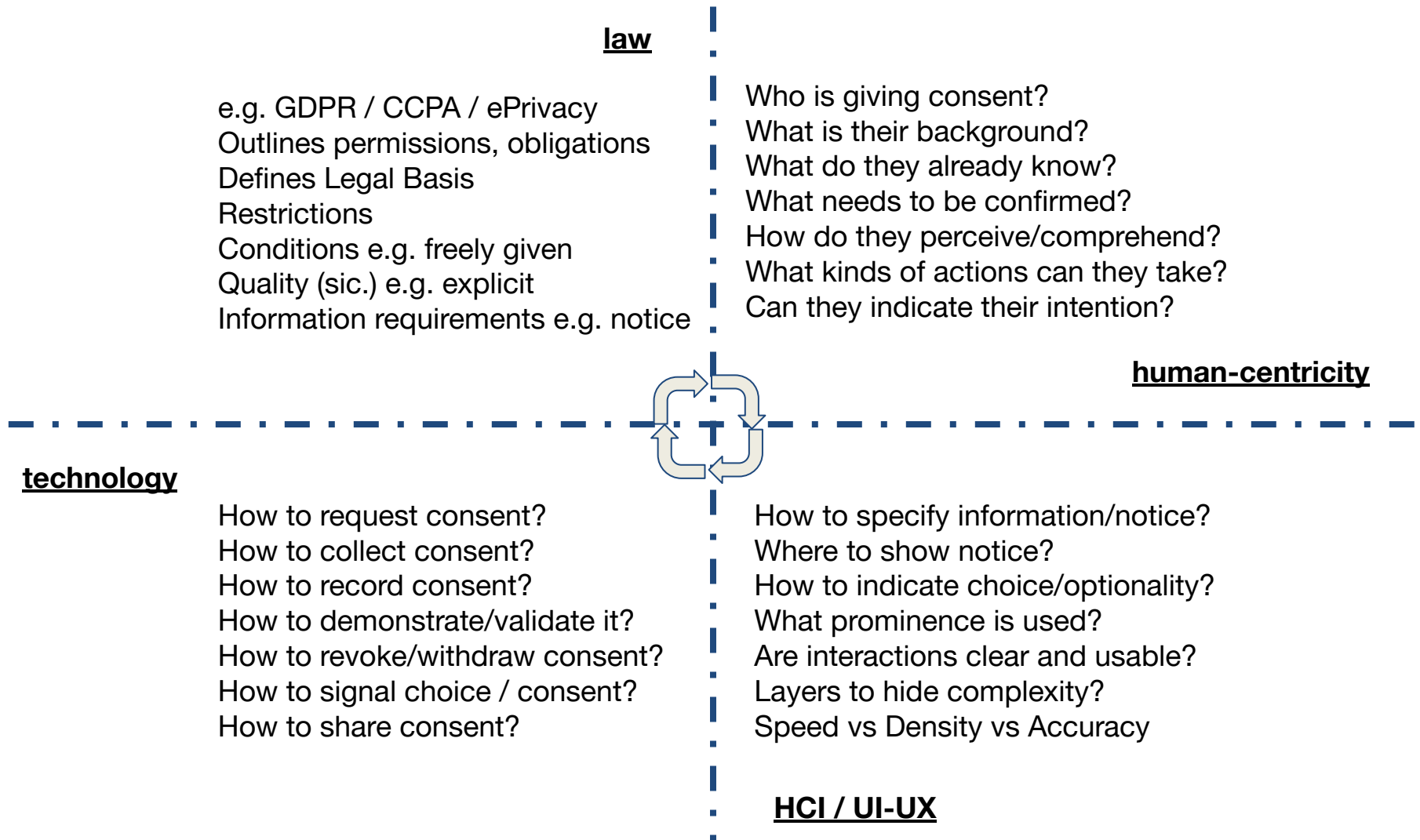
Technical and Org. Measures

Risks envisioned (sic.)

Automated Decision Making

Novel technologies

Profiling / Surveillance (sic.)



Dark Patterns (<https://www.darkpatterns.org/>)

Dark Patterns are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something.

- Nouwens et al. (2020) scraped five most popular consent dialogue providers on top 10,000 UK websites and found that **dark patterns and implied consent are the norm** – while only 11.8% of the website analysed were GDPR compliant.
- Human and Cech (2020) investigated sociological dimensions of consent and found GAFAM policies contained several **variations of dark patterns in interaction design, visual design and textual descriptions** of notices / requests for consent.
- Matte et al. (2020) list dark patterns within the IAB framework – largest ad networks on the internet – and showed that **websites do not respect consent choices and collect data anyway** regardless of what the users chose / indicated.
- Santos et al. (2020) expand on the above work and show (opine) “it’s **not possible to fully assess compliance with the law for the majority of requirements** because of the current architecture of the Web”

**Do Not Track (DNT)** → boolean (set on / off) browser signal to indicate user does not want to be 'tracked' across the websites. Last standardisation via W3C in 2019. All browsers implement it. No websites it. Spectacular failure.

<https://www.w3.org/TR/tracking-dnt/>

**Global Privacy Control (GPC)** → boolean (set on / off) browser signal to indicate user does not want their data to be 'shared' beyond the website/controller. Last specification Jan 2021. Only 1 browser currently implements it - Brave. Some websites support it. Legally enforceable under CCPA. Uncertain regarding GDPR<sup>1</sup>.

<https://globalprivacycontrol.github.io/gpc-spec/>

**Privacy Labels** → Apple introduced notices for its App Store which requires developers to post information about data collected and used for tracking of individuals, in addition to requiring them to ask consent for tracking - and provides a global setting to prohibit such requests. The company dogfoods: <https://www.apple.com/privacy/labels/>

<sup>1</sup> GPC + GDPR: will it work?. Harshvardhan J. Pandit. 2021. <https://harshp.com/research/blog/gpc-gdpr-can-it-work>



Kantara published **Consent Receipt** (2018) specification outlining a schema for issuing 'receipts' for given consent. Barebones spec, does not meet (any? most?) legal requirements.

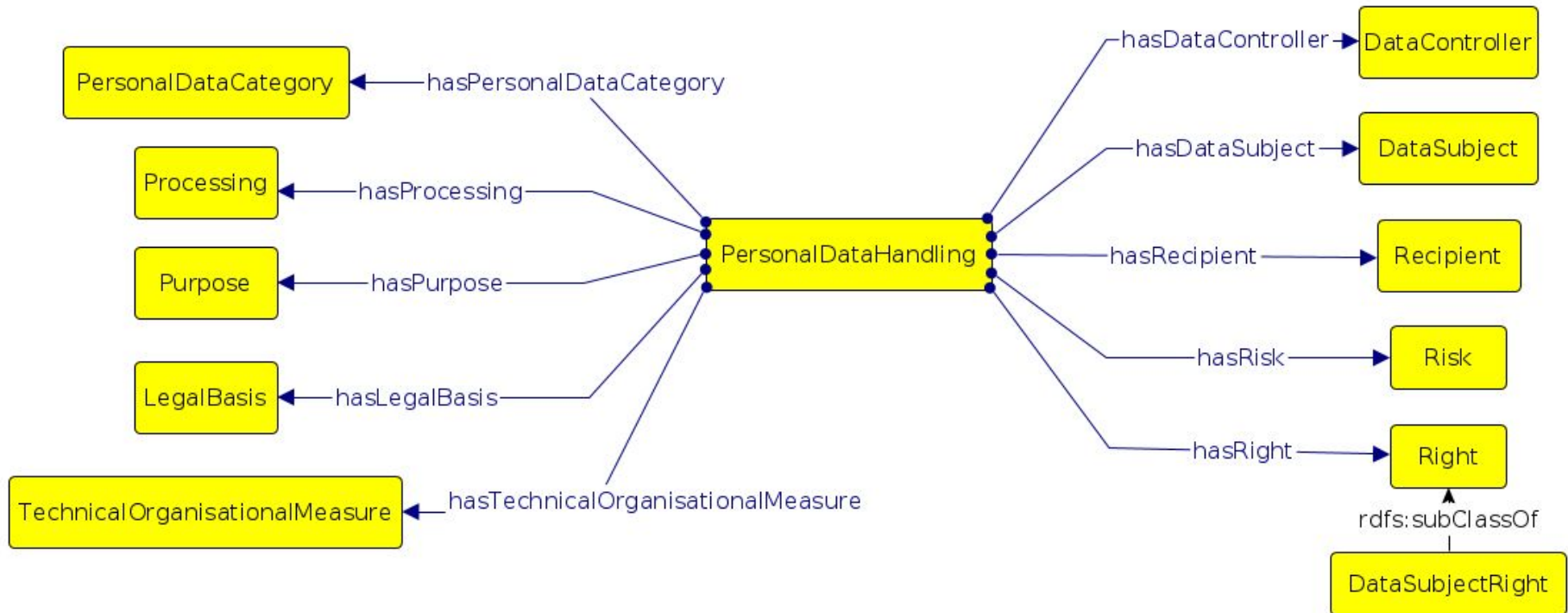
ISO/IEC published **29184** (2020-06) standard for online privacy notices for consent which involves requirements for consent dialogues and mentions possibility of machine-readable metadata.

Re:29184 - it requires asking explicit consent for some cases. But its definition of 'explicit consent' does not meet GDPR's requirements<sup>1</sup>.

ISO/IEC announced **27560** (likely publication >2023) as an upcoming standardisation effort for consent receipts. Data Protection Authorities involved via national standardisation bodies.

<sup>1</sup> Comparison of notice requirements for consent between ISO/IEC 29184:2020 and GDPR (Forthcoming). Harshvardhan J. Pandit\*, Georg Philip Krog\*. Journal of Data Protection & Privacy. 2021. <https://doi.org/10.5281/zenodo.4444925>

## Data Privacy Vocabulary<sup>1</sup> (DPV), v0.2, 2021 <https://w3.org/ns/dpv>



Machine-readable vocabulary for creation of technological solutions and enhancing interoperability

(A) Existing information → DPV

e.g. NLP<sup>2</sup> to analyse privacy policies → extract terms → perform legal analysis

(B) DPV → Generate Information

e.g. Utilise DPV to generate common ROPA<sup>3</sup> documentation for GDPR compliance

<sup>1</sup> Creating A Vocabulary for Data Privacy (alt: Data Privacy Vocabulary (DPV)). Pandit, Polleres et al. 2019. <https://zenodo.org/record/3934476>

<sup>2</sup> The Role of Vocabulary Mediation to Discover and Represent Relevant Information in Privacy Policies. Leone et al. 2020 <https://ebooks.iospress.nl/volumearticle/56164>

<sup>3</sup> A Common Semantic Model of the GDPR Register of Processing Activities. Ryan et al. 2020 <https://doi.org/10.3233/FAIA200876>

## III. METHODS & POTENTIAL APPROACHES

**Sources of Information:** cookie/consent notices, privacy/other policies, reports, publications, opinions of domain-experts;

**Methodologies:** surveys, interviews, focus groups, controlled and in-wild experiments, engagement with service providers, auditing, document analysis, data collection, data analysis;

**Technological aspects:** technological and algorithmic evaluation of benefits and their provision in services;

**Legal compliance:** conformance with legal frameworks;

**Legal rights:** rights provided by existing laws regarding benefits and information, e.g. Right to Access (GDPR A.15);

**Information transparency:** accessibility, availability, comprehensibility of information about benefits and its applicability;

**Benefits within/across domains:** benefits in the context of their respective domains, e.g. personalisation for retail and for medicine can have different consequences;

**Linguistic aspects:** quality, formulation, sentiment, readability, and vocabulary used in descriptions;

**Users' perspective towards benefits:** knowledge, attitude, preferences in general and specific to domains/services;

**Users' perception when consenting:** assess comprehension of benefits when interacting with consent requests, e.g. if a purpose is a benefit, to whom, and in what context;

**Users' perception after consenting:** assess (immediate and long-term) comprehension of promised and received benefits;

**Service Provider perspective:** knowledge, attitude, perception, framing of service providers regarding benefits;

**Actors involved:** different parties involved and their relations;

**Representation:** UI/UX aspects, nudging, dark; patterns

**Other human-centric aspects:** heterogeneity, cognitive, collective, and contextual aspects [5] in relation to benefits.



## [How] Do Users Benefit From Giving Consent?

Harshvardhan J. Pandit\*, Soheil Human\*, Mandan Kazzazi\*


<https://zenodo.org/record/4601141> To be Presented at Workshop on Technology and Consumer Protection (ConPro) - co-located with IEEE Symposium on Security and Privacy (IEEE S&P)





- RISKY: Exploring Privacy Risks of Technologies using Knowledge Graphs
  - <https://harshp.com/research/projects/risky>
  - Funded by Irish Research Council for 2 years
  - Create a vocabulary of known risks (using DPV)
  - Associate risks with scenarios, technologies, concepts
  - For 'new' situation, discover risks from existing knowledge
- Privacy as Expected: Consent Gateway (PaE:CG)
  - <https://privacy-as-expected.org/>
  - Funded by EU H2020 NGI Trust grant for 9 months
  - Update Consent Receipt to GDPR / CCPA requirements
  - Browser extension + server component to generate receipts
  - Gateway: third-party notary 'signs' receipt as a witness



### COMMUNITY & BUSINESS GROUPS

**CURRENT GROUPS**

**REPORTS**


**ABOUT**

[Home](#) / Consent Community Group

## CONSENT COMMUNITY GROUP

The concept of consent plays an essential role in the use of digital technologies as an enabler of the individual's ownership, control, and agency. Regulations such as the GDPR assert this relationship by permitting use of consent as one of the possible legal bases for the lawful practice of data processing. Through this, obtaining consent is widely practised in the digital world, and can be perceived as an essential means to enable the individual's agency regarding the management and ownership of their personal data. While different legal frameworks specify various requirements and obligations regarding the legal validity of consent, which should be, e.g. valid, freely given, specific, informed and active; existing and ongoing research shows that the majority of people are not empowered to practice their digital right to privacy and lawful "consenting" due to various malpractices and a lack of technological means acting in the individuals' interest. This group aims to contribute towards the empowerment of humans concerning their rights of privacy and agency, by advocating interdisciplinary, pluralist, human-centric approaches to digital consent that are technologically and legally enforceable. The mission of this group is to improve the experience of digital "consenting" while ensuring it remains adherent to relevant standards and laws. For this, the group will: (i) provide a space for people and stakeholders to come together (ii) highlight and analyse concepts, issues and problems about digital consenting (iii) propose and develop solutions. Some concrete areas for the working of this group are: (a) developing interdisciplinary solutions; (b) documenting and achieving legal compliance; (c) improving the user experience; and (d) utilising existing and developing new concepts and standards for digital consent.

Group's public email, repo and wiki activity over time



2020  
2021 J F M A M J J A S O N D

*Note: Community Groups are proposed and run by the community. Although W3C hosts these conversations, the groups do not necessarily represent the views of the W3C Membership or staff.*

### No Reports Yet Published

Chairs, when logged in, may publish draft and final reports. Please see [report requirements](#).

**PUBLISH REPORTS**


**Tools for this group**


- Mailing List
- IRC
- RSS
- Contact This Group

**Get involved**

Anyone may join this Community Group. All participants in this group have signed the W3C Community Contributor License Agreement.








**JOIN OR LEAVE THIS GROUP**




**Harshvardhan J. Pandit**

**Soheil Human**

*Chairs*

**Participants (26)**





[View all participants](#)

## Consent: Where are we going?

- ★ Legal Requirements
- ★ Notices and Information
- ★ UI / UX → Dark Patterns
- ★ Multidisciplinary approach
- ★ Existing research and State of the Art
- ★ Technological signalling of choice/preference
- ★ Standardisation
- ★ Metadata / Data Privacy Vocabulary
- ★ Consumer Protection
- ★ Consent Receipts
- ★ Community Groups