

Mirror Mirror on the Wall...

Why Must I Always Click on “Accept All” ???

Part II

Harshvardhan J. Pandit | pandith@tcd.ie | @coolharsh55
What Is the Internet Doing to Me? | 22 November 2022 | Trinity College Dublin
Slides available at: <https://harshp.com/research/presentations>

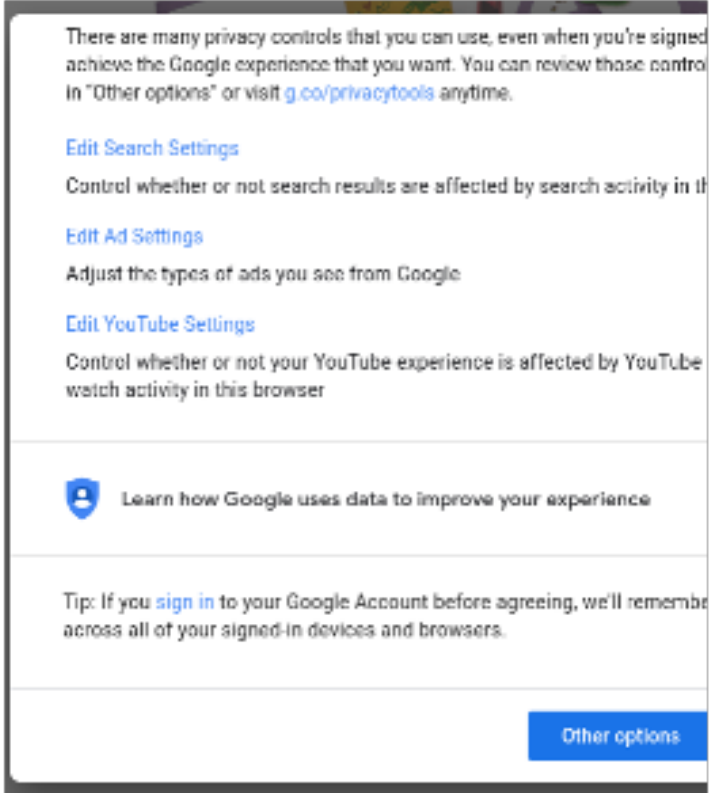
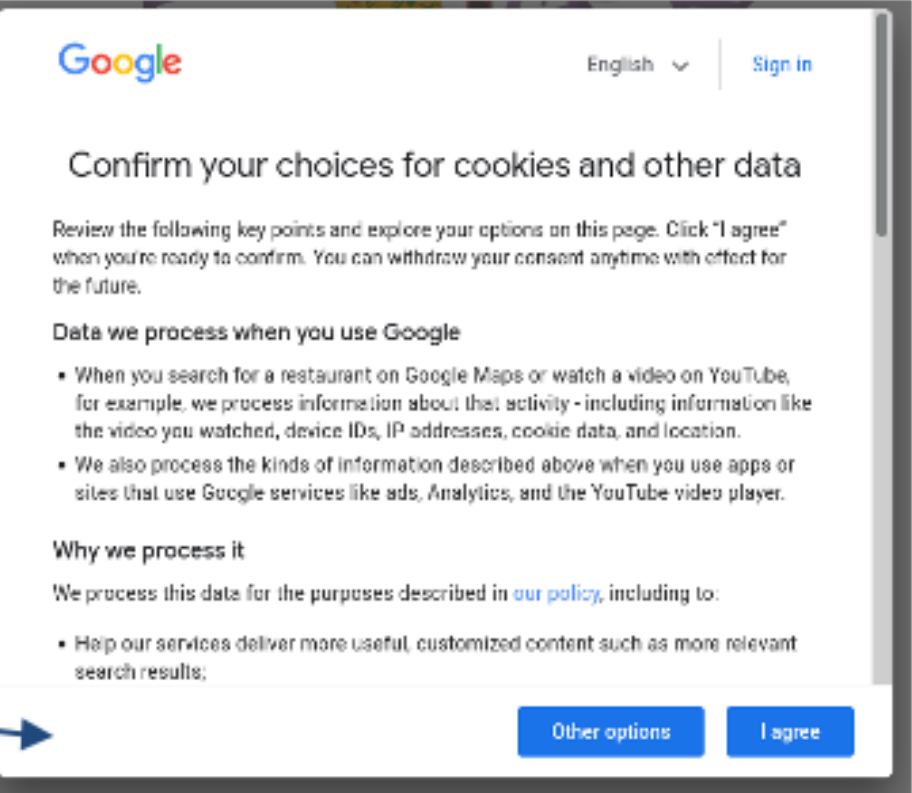
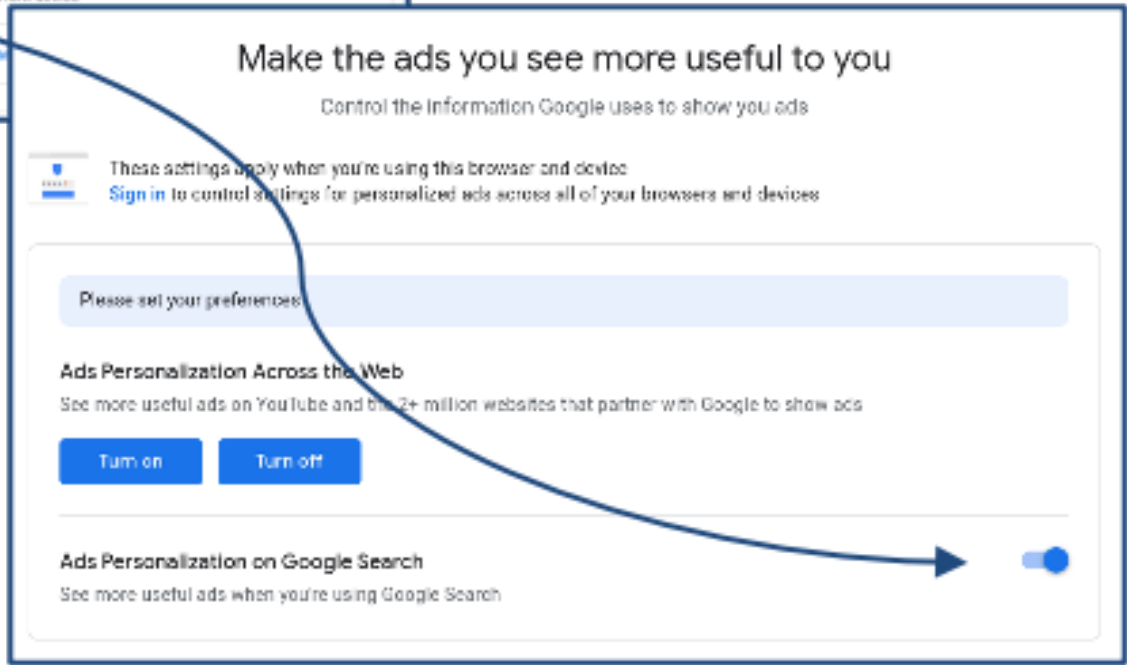
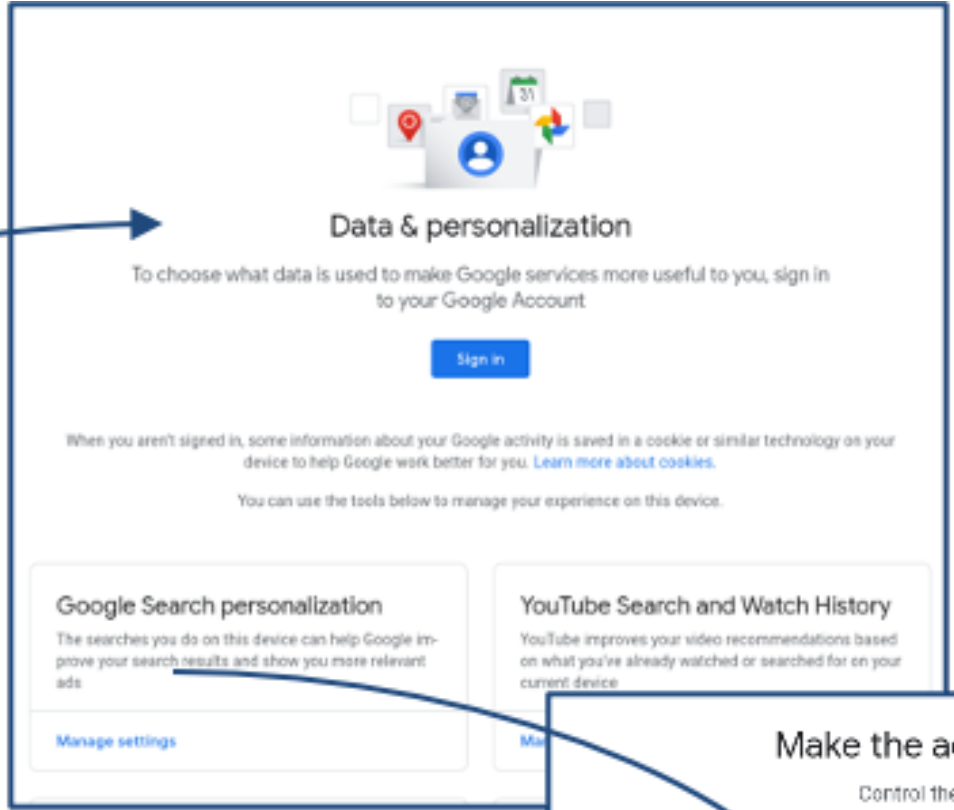
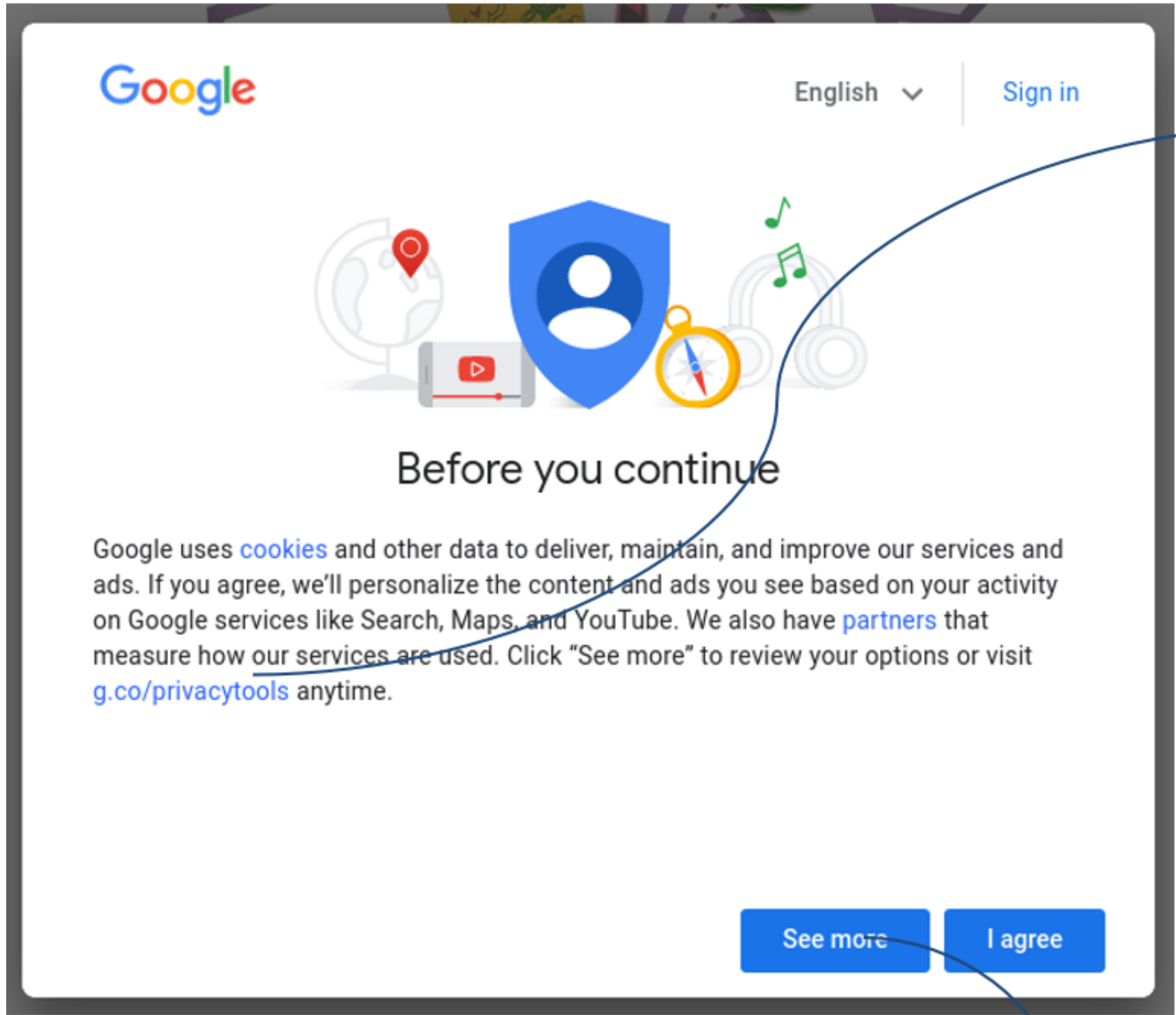
Ever visited a website and got blocked by a popup?

Was it annoying?

Why was it there?

What do you think is the quickest way to get rid of it?





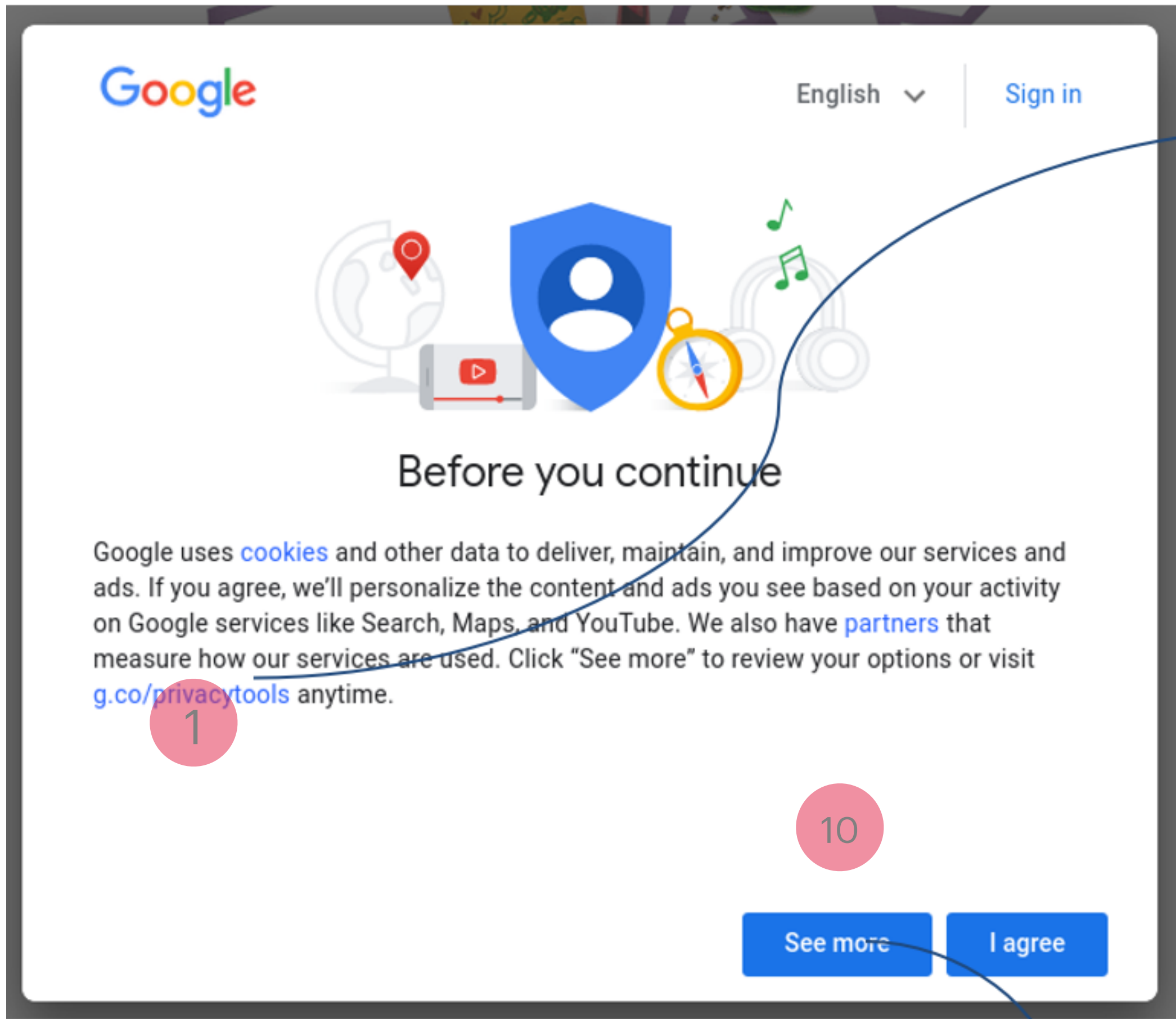
Companies are required to show you a “NOTICE” informing what data they collect and how they use it.

Where this is based on your CONSENT, they need to ask your permission before they can proceed.

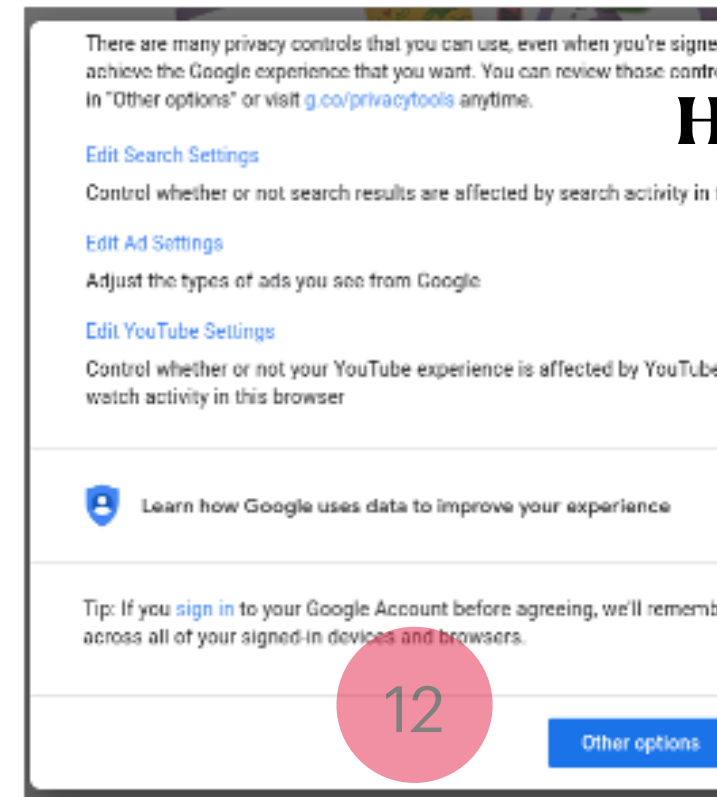
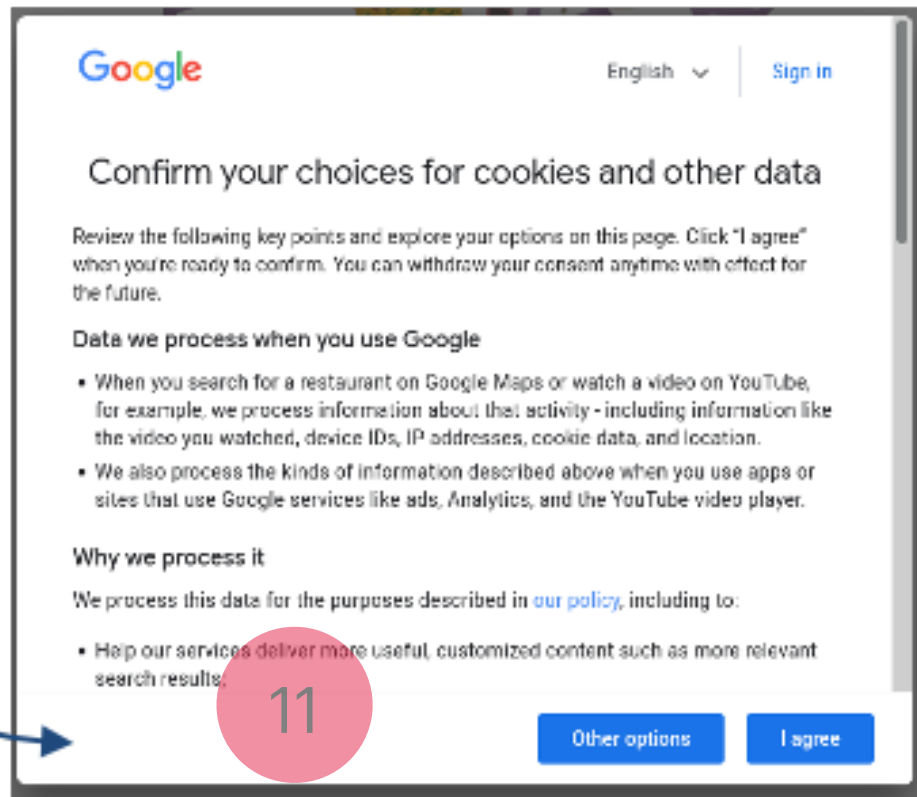
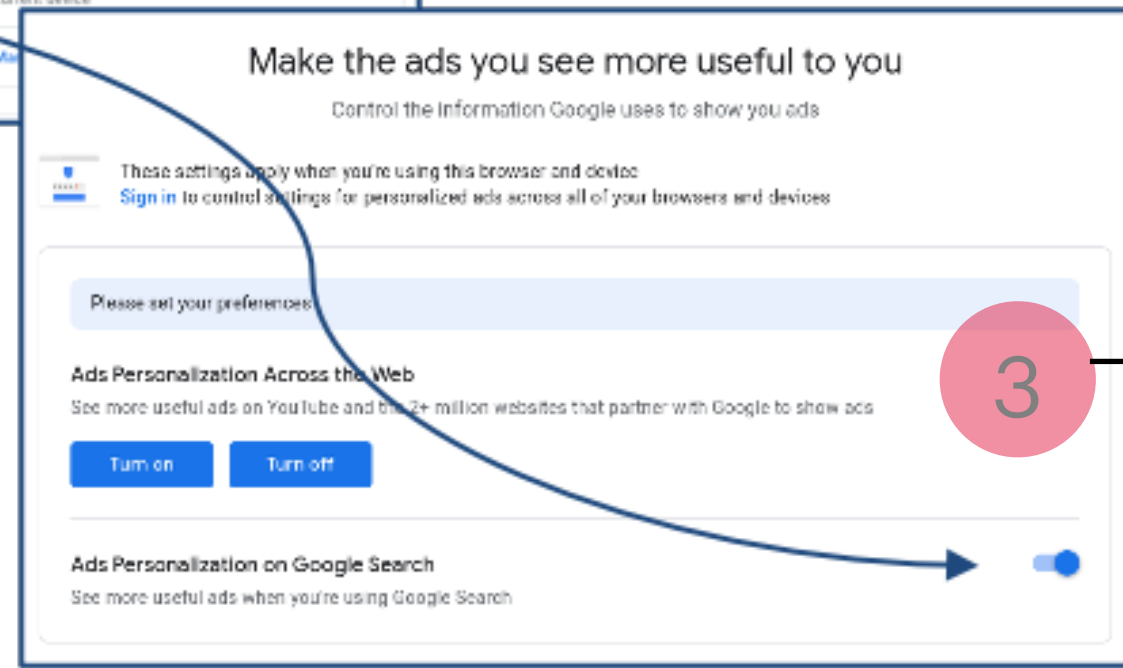
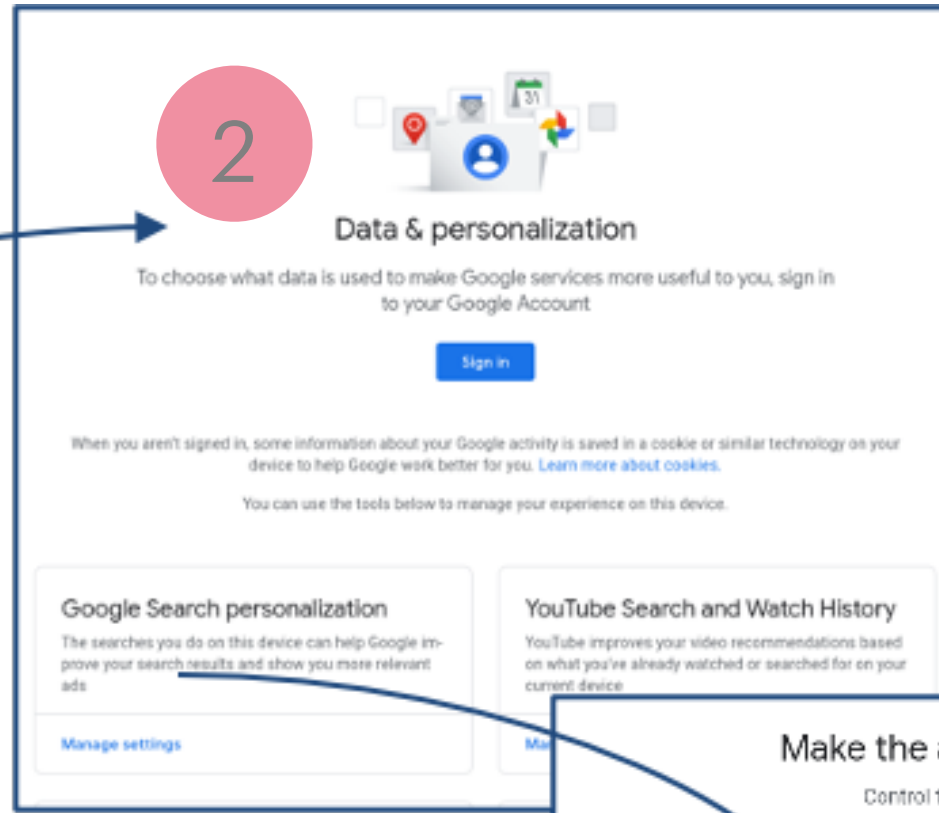
Since every website visit collects and uses your personal data, this means there's a notice & consent process every time you visit a website ...



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



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



Companies are required to show you a “NOTICE” informing what data they collect and how they use it.

Where this is based on your CONSENT, they need to ask your permission before they can proceed.

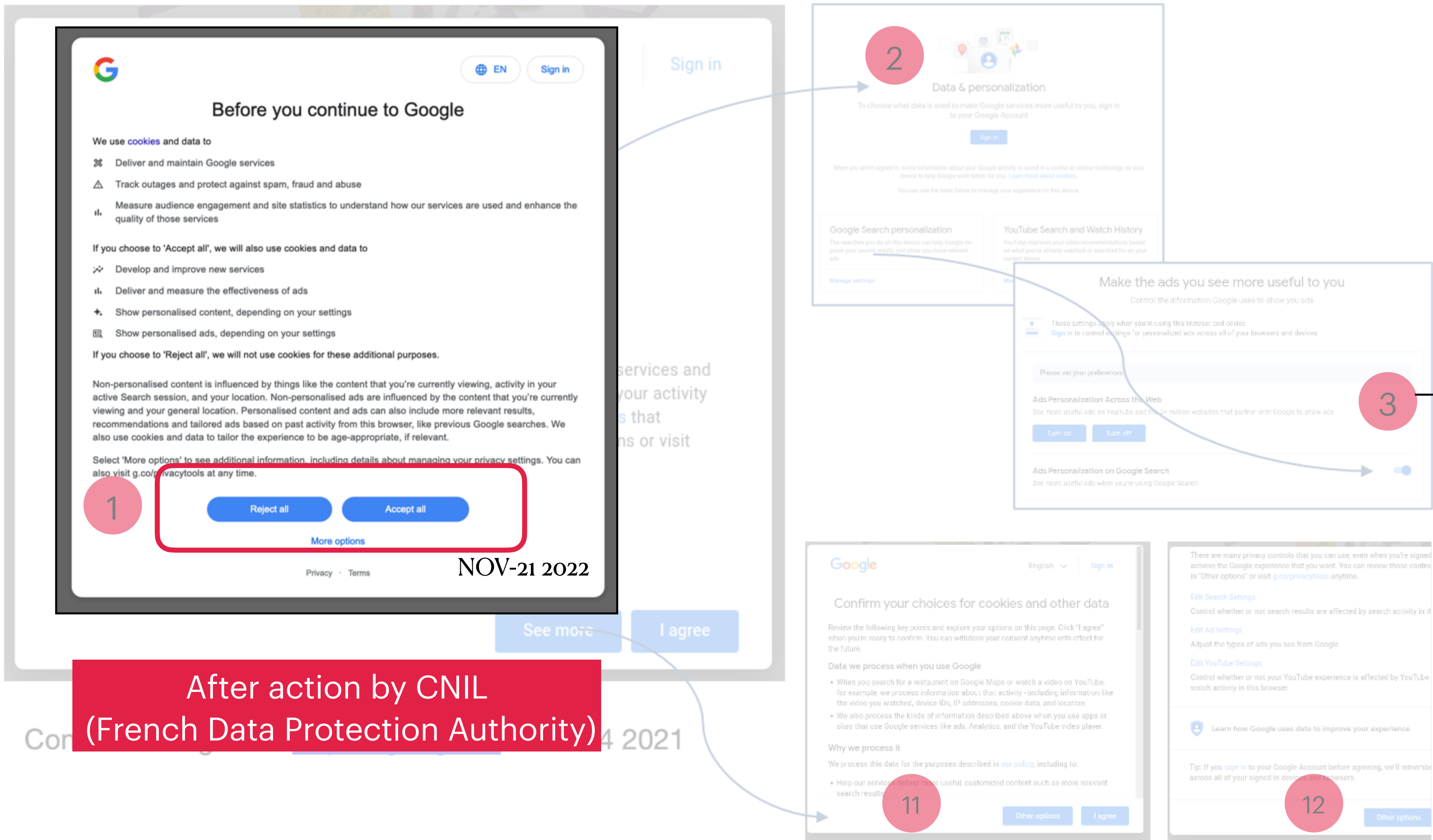
Since every website visit collects and uses your personal data, this means there’s a notice & consent process every time you visit a website ...

How many clicks to “Accept” ==> 1

How many clicks to “Reject” ==> 3

How many clicks to “Truly Reject” ==> 12

Do you think this is:
LEGAL ?
ETHICAL ?
NECESSARY ?



Companies are required to show you a “NOTICE” informing what data they collect and how they use it.

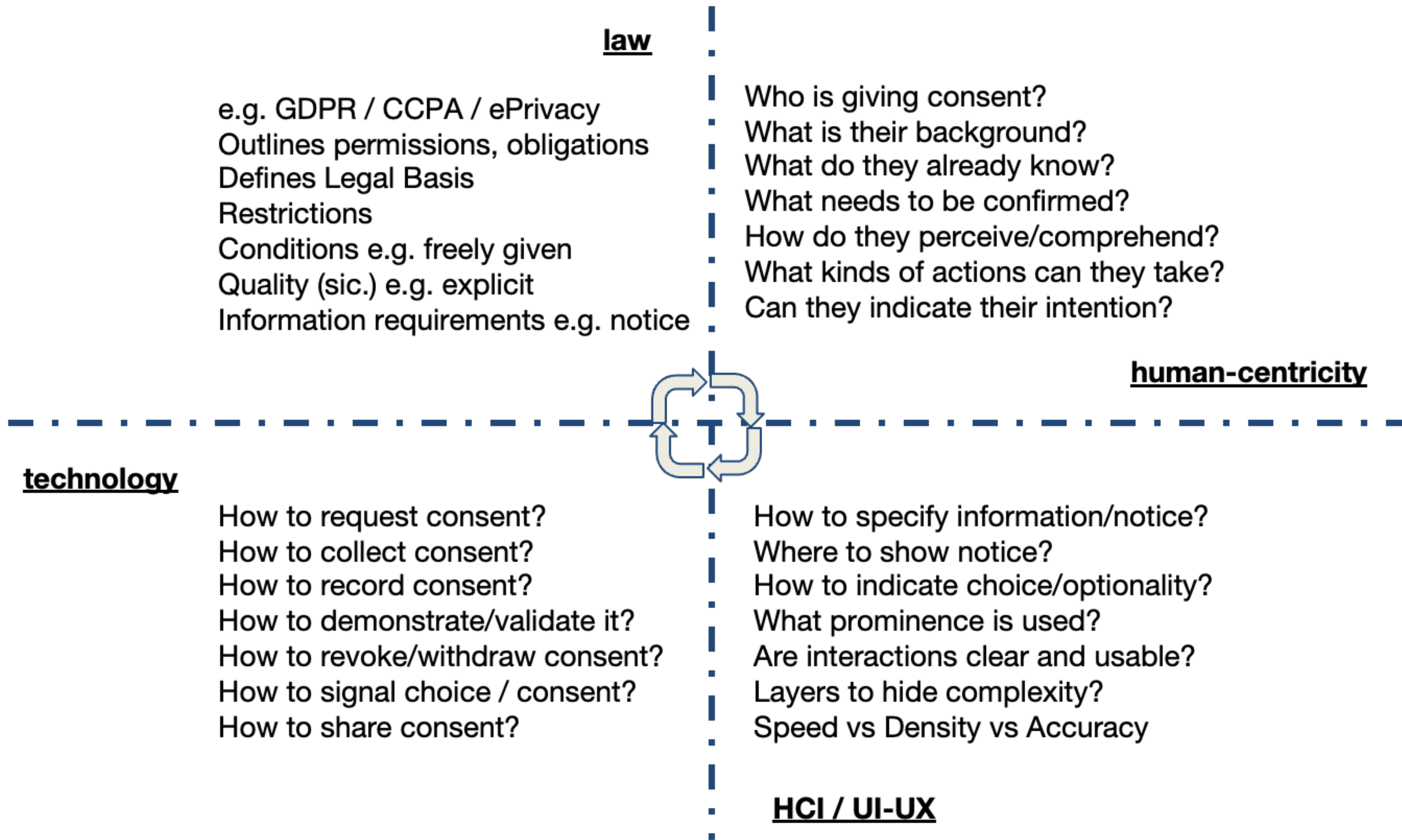
Where this is based on your CONSENT, they need to ask your permission before they can proceed.


Since every website visit collects and uses your personal data, this means there’s a notice & consent process every time you visit a website ...

How many clicks to “Accept” ==> 1

How many clicks to “Reject” ==> 2

Hidden Gotches ? Several





Quantcast

Data Controller

We value your privacy

Third Party

We and our **partners** store and/or access information on a device, such as **cookies** and process personal data, such as **unique identifiers** and standard information sent by a device for **personalised ads** and content, ad and content measurement, and audience insights, as well as to develop and improve products.

Technology

Purpose

Personal Data Category

With your permission we and our partners may use **precise geolocation data and identification** through device scanning. You may click to consent to our and our partners' processing as described above. Alternatively you may click to **refuse to consent** or access more detailed information and change your preferences before consenting.

Legal Basis = Consent

Please note that some processing of your personal data may not require your consent, but you have a right to object to such processing. Your preferences will apply to this website only. You can **change your preferences** at any time by returning to this site or visit our privacy policy.

Right to Withdraw Consent

Disagree? Refuse Consent?

DISAGREE

Options for ...?

MORE OPTIONS

Agree to statement ? Give Consent ?

AGREE

<https://www.quantcast.com/> THU 17 NOV 2021

What is your first impulse to do here?
 What button do you think you would have clicked?
 What button do you think most people click?

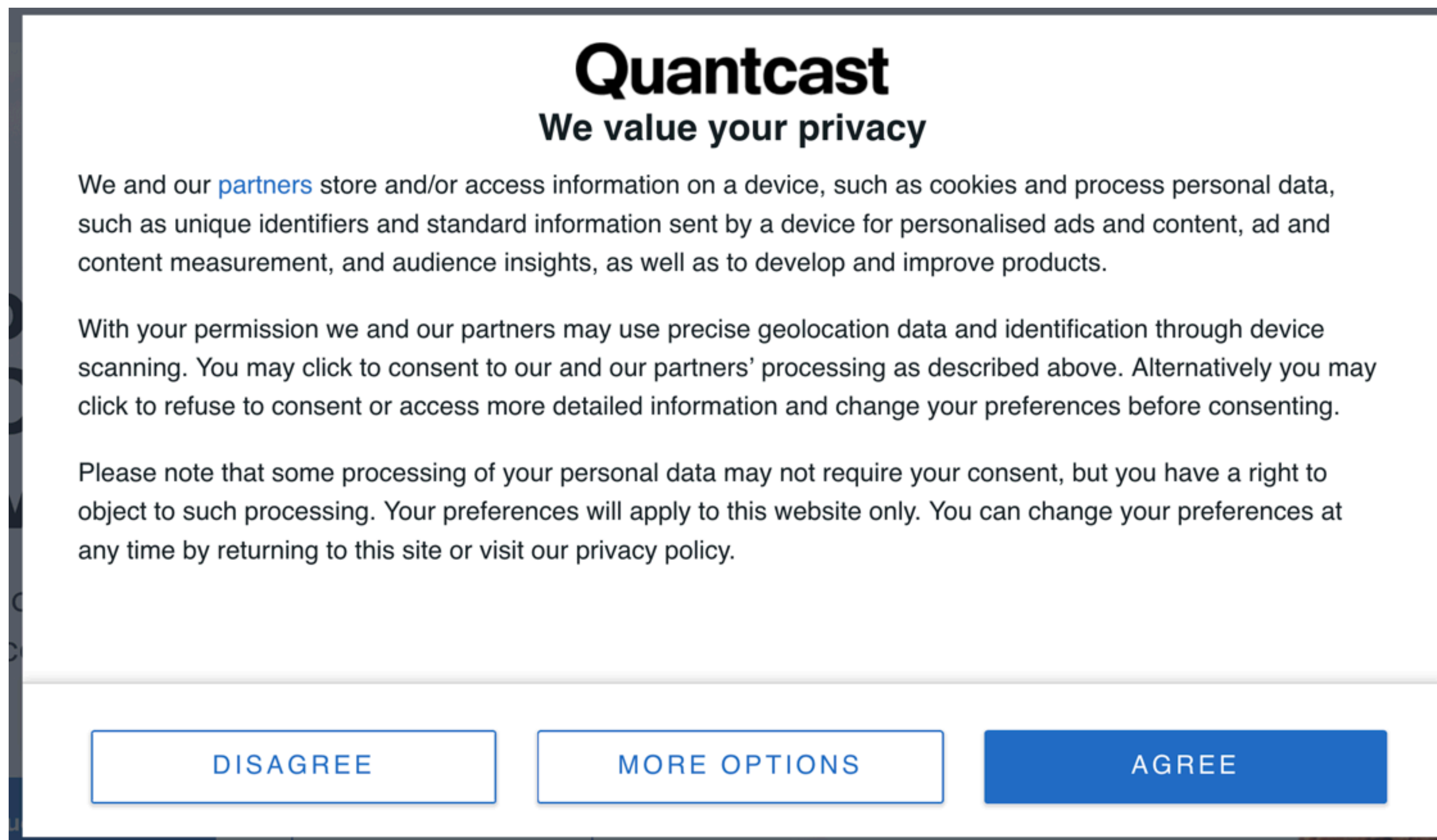
GDPR Art 4, 7, 13, 14

Information to be provided in a “Notice”

- 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.)

Consent should be:

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



1. The button for “giving consent” is differently styled than the one for “refusing consent”
2. A person is more likely to click on the “brighter” styled button i.e. “Agree”
3. This is because we have been primed to interact with digital interfaces consisting of such design choices on computers, smartphones, switches, machinery ...
4. This creates an unfair situation where a person is enticed to give away their consent and personal data
5. Through this, companies manipulate people into clicking “accept” even when they have not read or understood what they agreeing to
6. This results in an unfair choice !

This is called a “Dark Pattern”

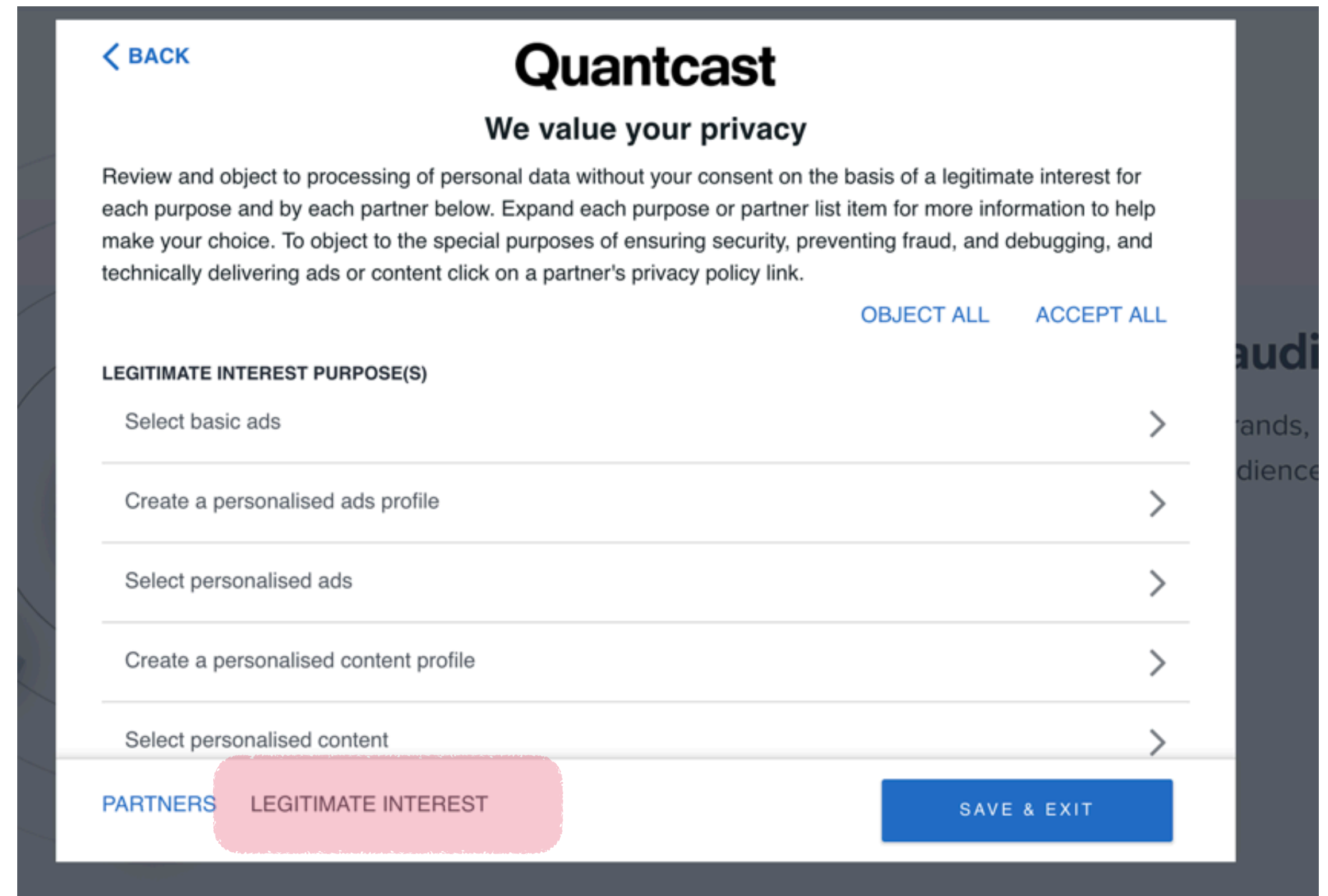
Have you seen similar manipulations elsewhere? Can you recall some examples? Are you aware of being manipulated?

<https://www.quantcast.com/> THU 17 NOV 2021

Even if you click “Disagree” ...

LEGITIMATE INTEREST

Basically, a “FU, I’ll do whatever I want” situation by companies ...



The screenshot shows the Quantcast privacy settings interface. At the top, there is a 'BACK' link and the Quantcast logo. Below the logo, the heading 'We value your privacy' is displayed. A paragraph explains the legitimate interest basis for processing personal data. To the right of this paragraph are links for 'OBJECT ALL' and 'ACCEPT ALL'. The main section is titled 'LEGITIMATE INTEREST PURPOSE(S)' and contains a list of five items, each with a right-pointing chevron: 'Select basic ads', 'Create a personalised ads profile', 'Select personalised ads', 'Create a personalised content profile', and 'Select personalised content'. At the bottom, there are three buttons: 'PARTNERS' (blue), 'LEGITIMATE INTEREST' (pink, highlighted with a red box), and 'SAVE & EXIT' (blue).

More Dark Patterns ...!

Go to <https://www.darkpatterns.org/> for a comprehensive overlook

I collect academic literature on dark patterns here: <https://www.zotero.org/hpandit/collections/WXB75TJ5>

- Burden with too many choices
- Use design to entice one option over another
- Easier to select one option than another
- Block you from using until you give consent
- Keep asking again and again ...
- Use opt-out instead of opt-in



Is this even Legal ...?

You ask, I say NO, the authorities haven't said much anyway ...

- Yes, this is not valid as per the GDPR requirements
- Why hasn't it been fixed?
- Because EU has an enforcement problem !
- A Data Protection Authority or Supervisory Authority is responsible for investigating such issues. BUT
 - They are under-funded
 - Court proceedings take time
 - They are reluctant to carry out partial investigations (it seems)
 - This is a L A R G E scale problem - millions of websites probably

Sometimes it outright illegal !!!

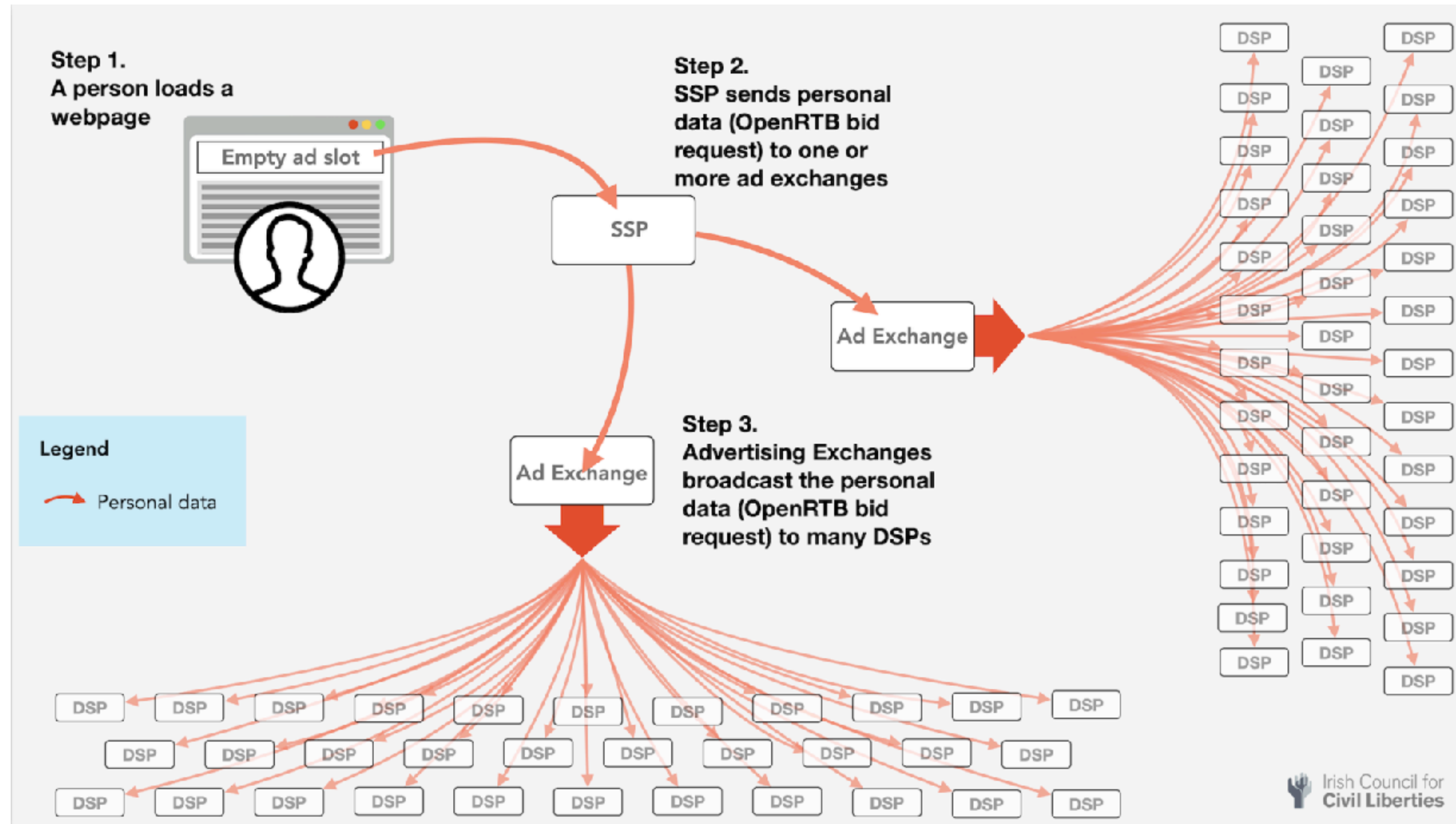
- Consent “assumed” even before you make a choice [1]
- Consent “assumed” even if you click disagree [1]
- Incorrect use of legal base e.g. use Legitimate Interest instead of consent [2]
- Collect consent for ~1000 third parties with a single click [2]
- Make it difficult to withdraw consent [2]
- Keep fighting court cases instead of fixing obviously illegal practices [3]

[1] For example, see Nouwens, Midas, et al. "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*. 2020. <https://people.csail.mit.edu/ilaria/papers/Midas-MITCHI2020.pdf>

[2] Matte, Célestin, Nataliia Bielova, and Cristiana Santos. "Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework." 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020. <https://hal.inria.fr/hal-03117294/document>

[3] See investigation reports and documents published regarding WhatsApp v DPC Ireland and Facebook/Meta v DPC Ireland (2021)

Personalised Advertising via Real-Time Bidding



<https://www.iccl.ie/digital-data/iab-europe-cant-audit-what-1000-companies-that-use-its-tcf-system-do-with-our-personal-data/>

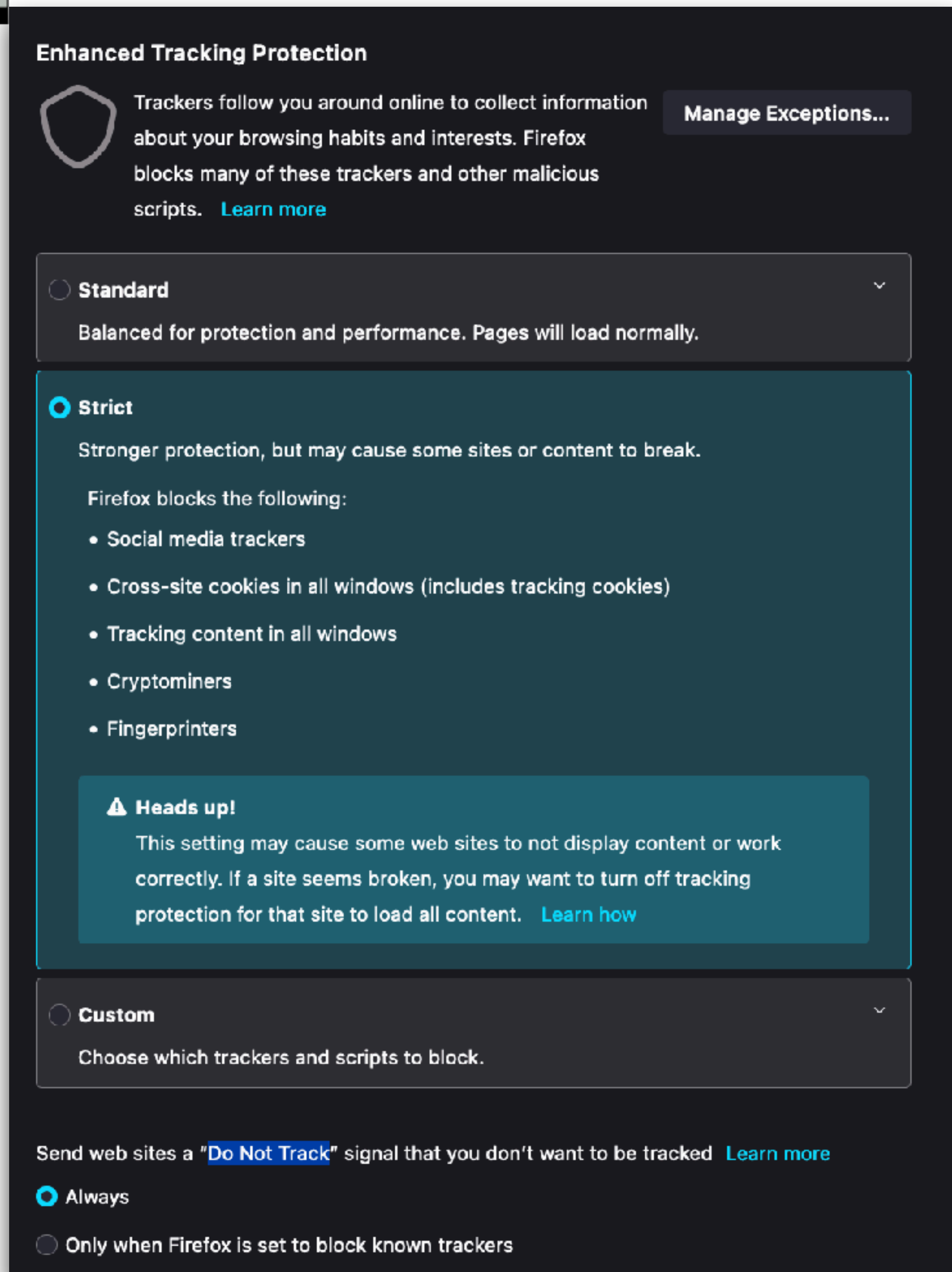
Overview of Personalisation Issues

Key takeaways

- What data is ‘used’ ??? —> Transparency
- What data is ‘needed’? What is ‘necessary’? —> Data Minimisation
- What are the sources of ‘data’ ? —> Transparency
- Is any data ‘sensitive’ ? Is it ‘special’ ? —> Ethical Concerns
- Is data (input/output) ‘accurate’ —> Accountability
- Is the output configurable ? —> Privacy by Design / Default
- Understand distinctions between *Privacy* vs *Security* vs *Identifiability* vs *Control*

Protecting Privacy

Techs, Tools, & Approaches



DNT: Do Not Track

Privacy Signals of the Past

- A relatively “simple” boolean signal (set / not set)
- Sent with every web communication as a preference/signal
- Indicated to websites/companies whether to track you or not
- Standardised (kind of) as a specification
- Supported by all Major Browsers
- Lots of disagreements on what “tracking” should mean
- Seemed like a great idea on the precipice of bringing change

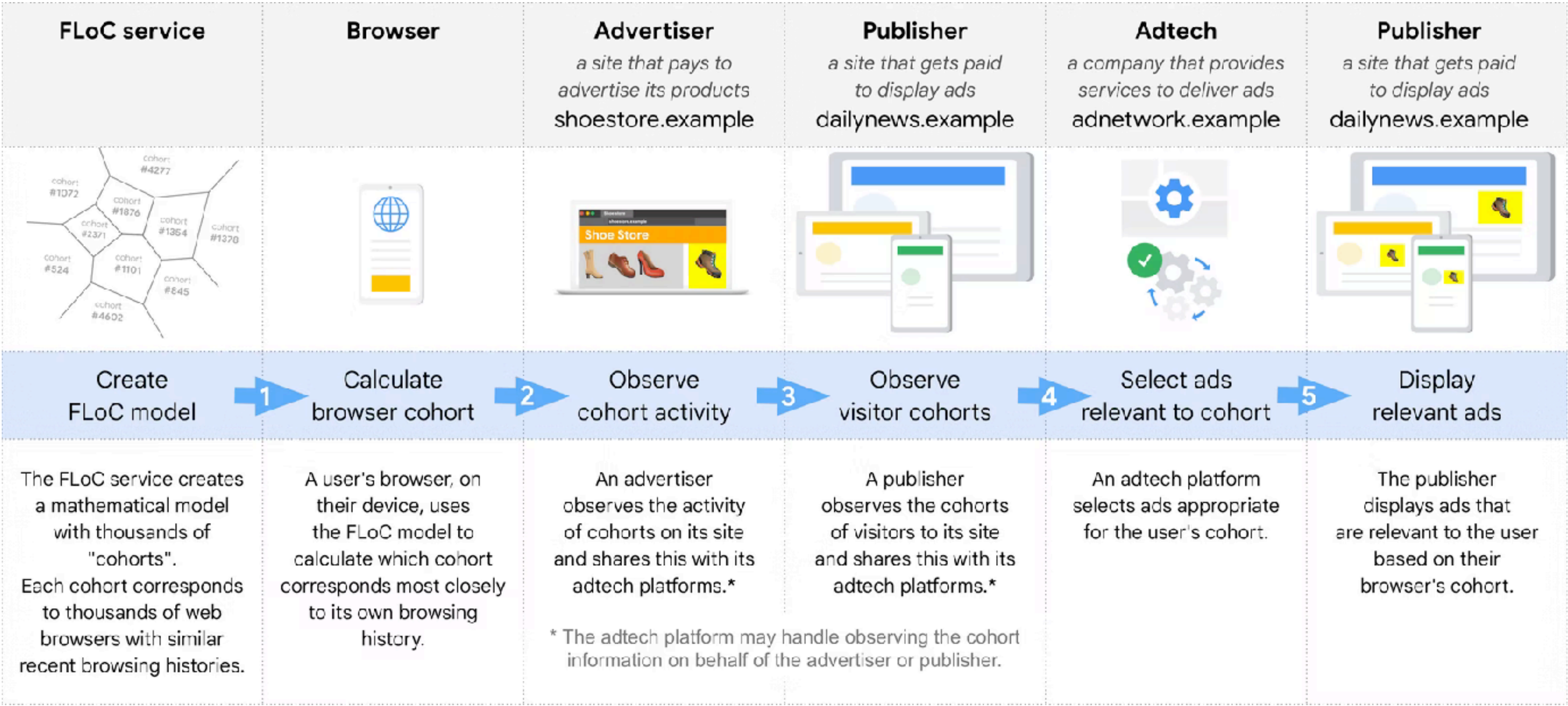
Seemed great until ...

- Microsoft made it SET/ON by default in Internet Explorer
- Debates, fights, and discussions ensued
- Long story short, it got killed. Hard.
- Even though most browsers still allow setting this signal, websites don't respect and neither do the authorities seem to consider this a valid signal

Wikipedia actually has a great summarised version of the events: https://en.wikipedia.org/wiki/Do_Not_Track

Google’s FLoC Proposal

Federated Learning of Cohorts



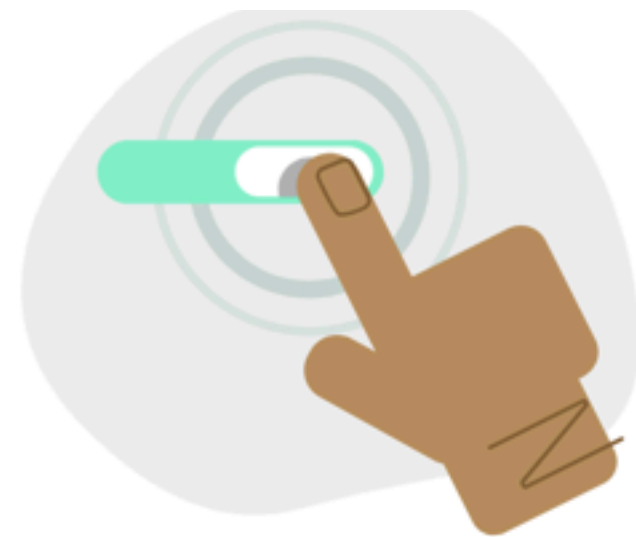
<https://developer.chrome.com/docs/privacy-sandbox/floc/>

Global Privacy Control (GPC)

Privacy Signals of the Present

EXAMPLE 1: Example GPC Request

```
GET /something/here HTTP/1.1
Host: example.com
Sec-GPC: 1
```



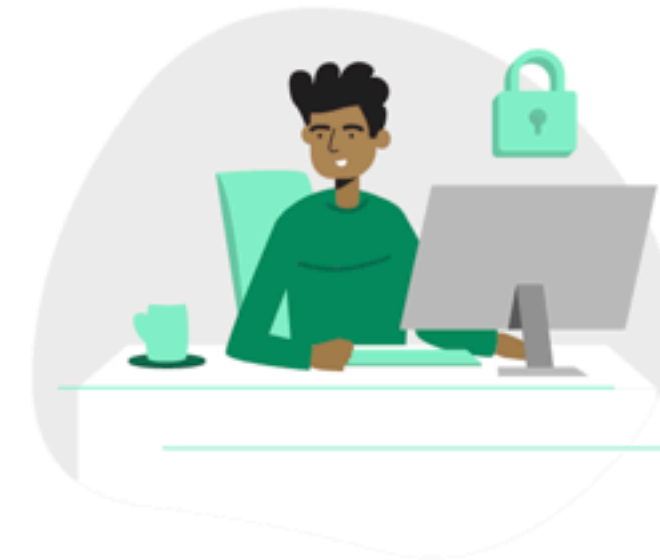
Turn On GPC

Enable Global Privacy Control to communicate your privacy preference.



Send the Signal

Your browser will send the GPC signal to websites you visit.










Exercise Your Rights

Participating websites can respect your privacy rights accordingly.

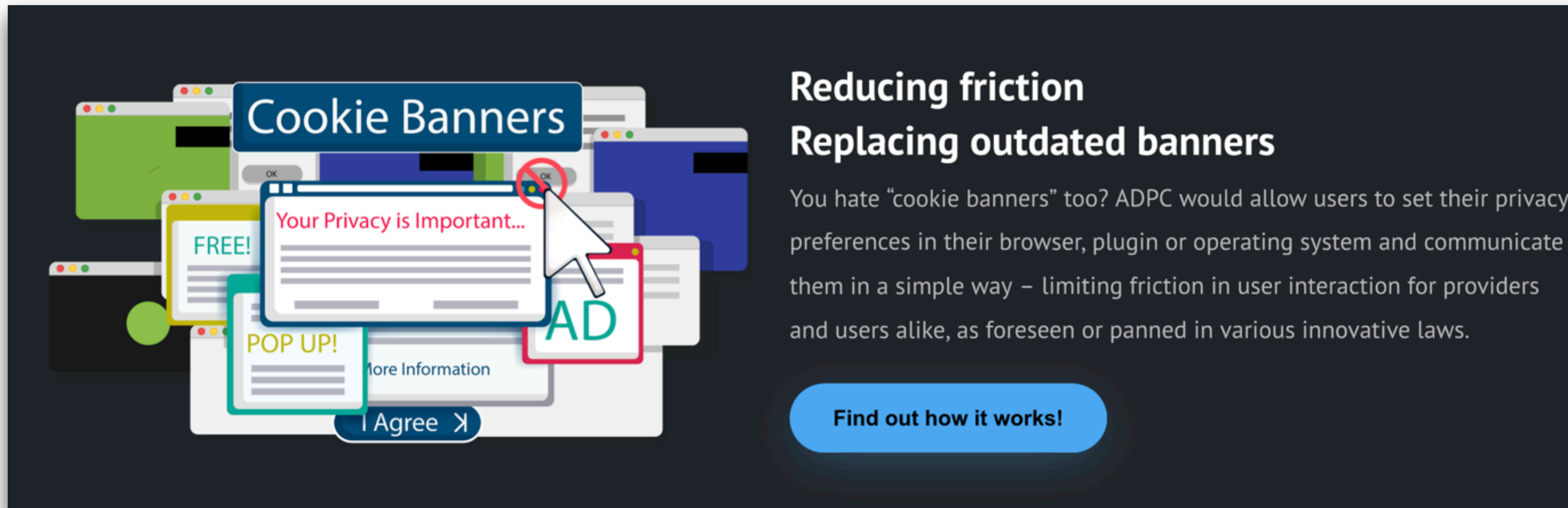
<https://globalprivacycontrol.org/>

DNT re-invented
Instead of “track”, its “sell” as per CCPA
Will this work with GDPR? Yet to be seen.

	Abine
	Brave Privacy Browser
	Disconnect
	DuckDuckGo Privacy Browser
	Firefox
	OptMeowt by privacy-tech-lab
	Privacy Badger by EFF

Advanced Data Protection Control (ADPC)

Privacy Signals of the Future?



Reducing friction
Replacing outdated banners

You hate “cookie banners” too? ADPC would allow users to set their privacy preferences in their browser, plugin or operating system and communicate them in a simple way – limiting friction in user interaction for providers and users alike, as foreseen or panned in various innovative laws.

[Find out how it works!](#)



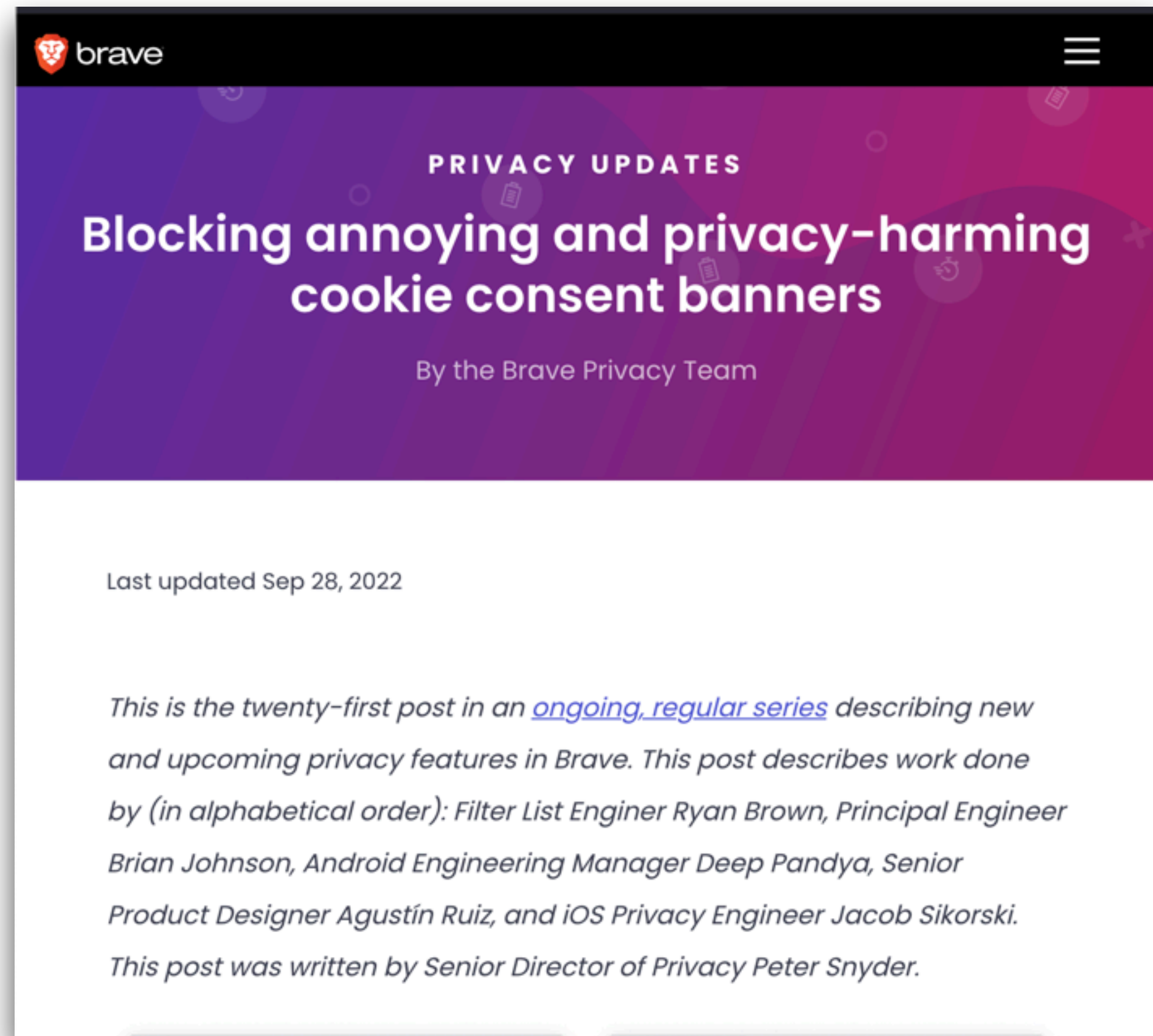
*My privacy is
none of your business*

<https://noyb.eu/en>

<https://www.dataprotectioncontrol.org/>

Seems like a spiritual successor to P3P, which allowed users to set privacy related preferences in a machine-readable format. Was deemed too complex, unpopular, difficult to implement, and project was shelved. <https://www.w3.org/P3P/>

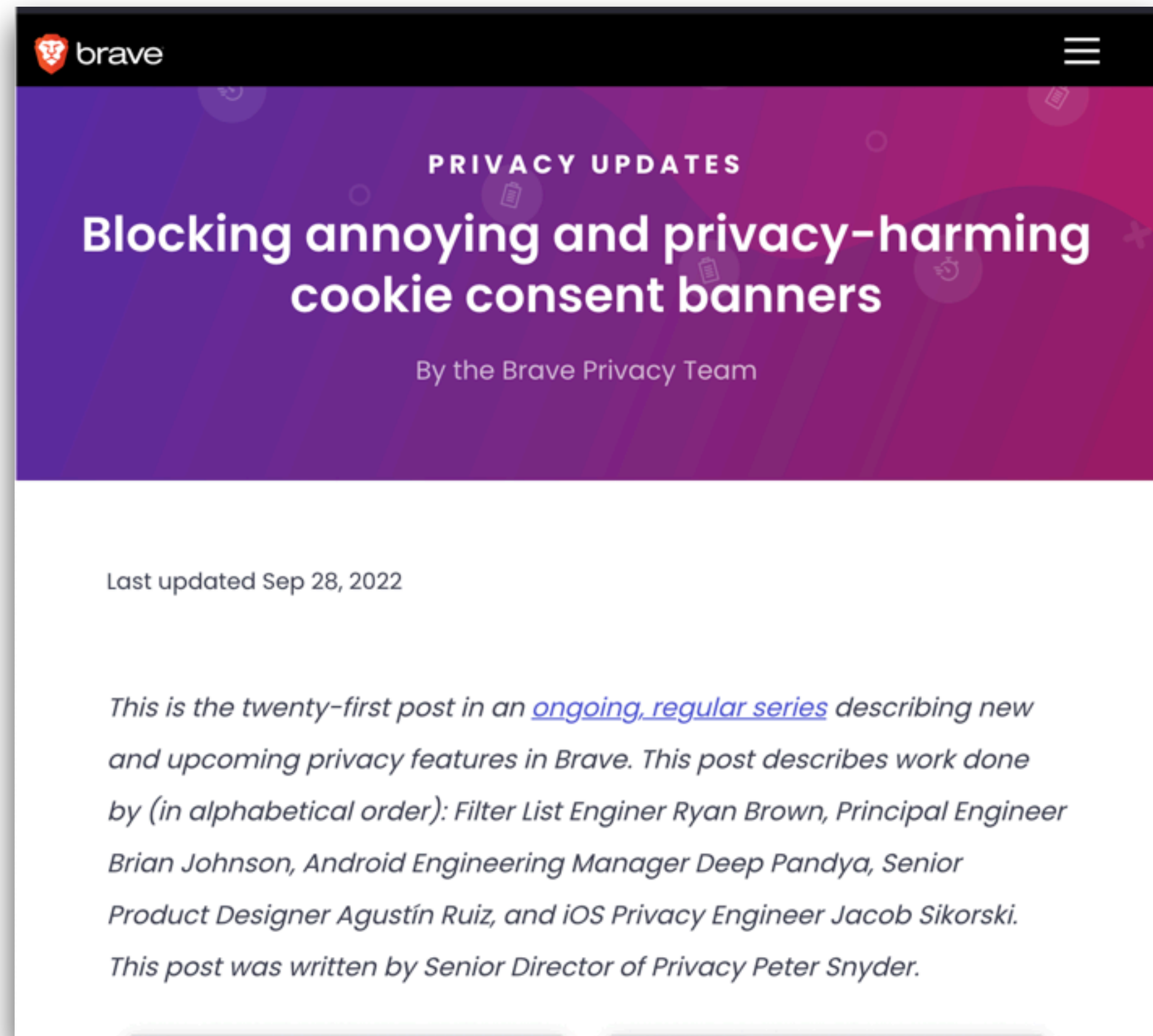
Brave - default blocking of Consent dialogues



By default - no consent dialogues, no pop-ups.
Is this Okay?
Do you foresee any issues?

<https://brave.com/privacy-updates/21-blocking-cookie-notices/>

Brave - default blocking of Consent dialogues



By default - no consent dialogues, no pop-ups.
Is this Okay?
Do you foresee any issues?

Gives convenience - no more annoying pop-ups
BUT
Not a good long term solution, because it 'hides'
what is actually happening and prevents you from
exercising what is your right —

- 1) to know what is happening;
- 2) to control your consent; and
- 3) to object to companies harvesting your data

<https://brave.com/privacy-updates/21-blocking-cookie-notices/>

Firefox - proposes auto-clicking reject/accept



What is Cookie Banners Handling?

Firefox now clears these annoying cookie banners on your behalf. We'll always hit "Reject all" if we have that option though in absence of a "Reject all" we'll do what you'd do otherwise and hit "Accept all"

Please help us test new features and give feedback on Cookie Banners handling! Join us in [#foxfooding](#) in [Matrix](#) to get more updates.

<https://community.mozilla.org/en/campaigns/firefox-cookie-banner-handling/>

Auto-REJECT? Good!
Auto-ACCEPT??? Illegal!

Similar to Brave, also gives convenience.

BUT

In this case, by auto-clicking "ACCEPT", you have given your consent. This is like leaving the door open because robbers might ruin the lock.

Also remember, GDPR requires consent to be an active action by you.

So you cannot automate giving consent!

Consent-O-Matic

Automate Rejection of Consent + Objection to Legitimate Interest

Consent-O-Matic

Nearly all websites use tracking technologies to collect data about you. By law, they often need your permission, which is why many websites have “consent pop-ups”. However, 90% of these pop-ups use so-called “dark patterns”, which are designed to make it very difficult to say no, but very easy to say yes. Although using dark patterns is illegal, the laws are not enforced enough, so many websites get away with it.

Consent-O-Matic is a browser extension that recognizes CMP (Consent Management Provider) pop-ups that have become ubiquitous on the web and automatically fills them out based on your preferences – even if you meet a dark pattern design. Sometimes a website might not use standard categories, and in that case, Consent-O-Matic will always try to submit the most privacy preserving settings.

Auto-REJECT? Good!
Auto-OBJECT? Awesome!

Consent-O-Matic is a browser extension that ‘automates’ the rejections and objections for popular CMP providers. Based on thorough GDPR research and analysis.

Probably the best ‘reactive’ solution.

<https://consentomatic.au.dk/>

Pro-active Solutions?

What can we develop using technology to make the internet a better place?

Share some ideas!

Pro-active Solutions?

What can we develop using technology to make the internet a better place?

- Privacy Policy - use NLP to parse information
- Visualisation and Summarisation e.g. policies
- Automate preferences & express them to avoid pop-ups
- Blockers for ads trackers/fingerprinting
- Use hardened secure browsers

Reactionary Solutions?

What can we do more using technology to change the way things are happening?

- Help legal investigations — join the dots from tech to law
- Provide automation potential e.g. information, actions
- Standardise terms, concepts, vocabularies
- Make complaining easier and more efficient

(I'm referring to legal complaints, but also applies to other things in life!)

SOLID: A Decentralised Web

<https://solidproject.org/>

Centralised

- Companies decide how to collect, store data
- Companies decide how/where to use it
- Companies offer you choices and controls

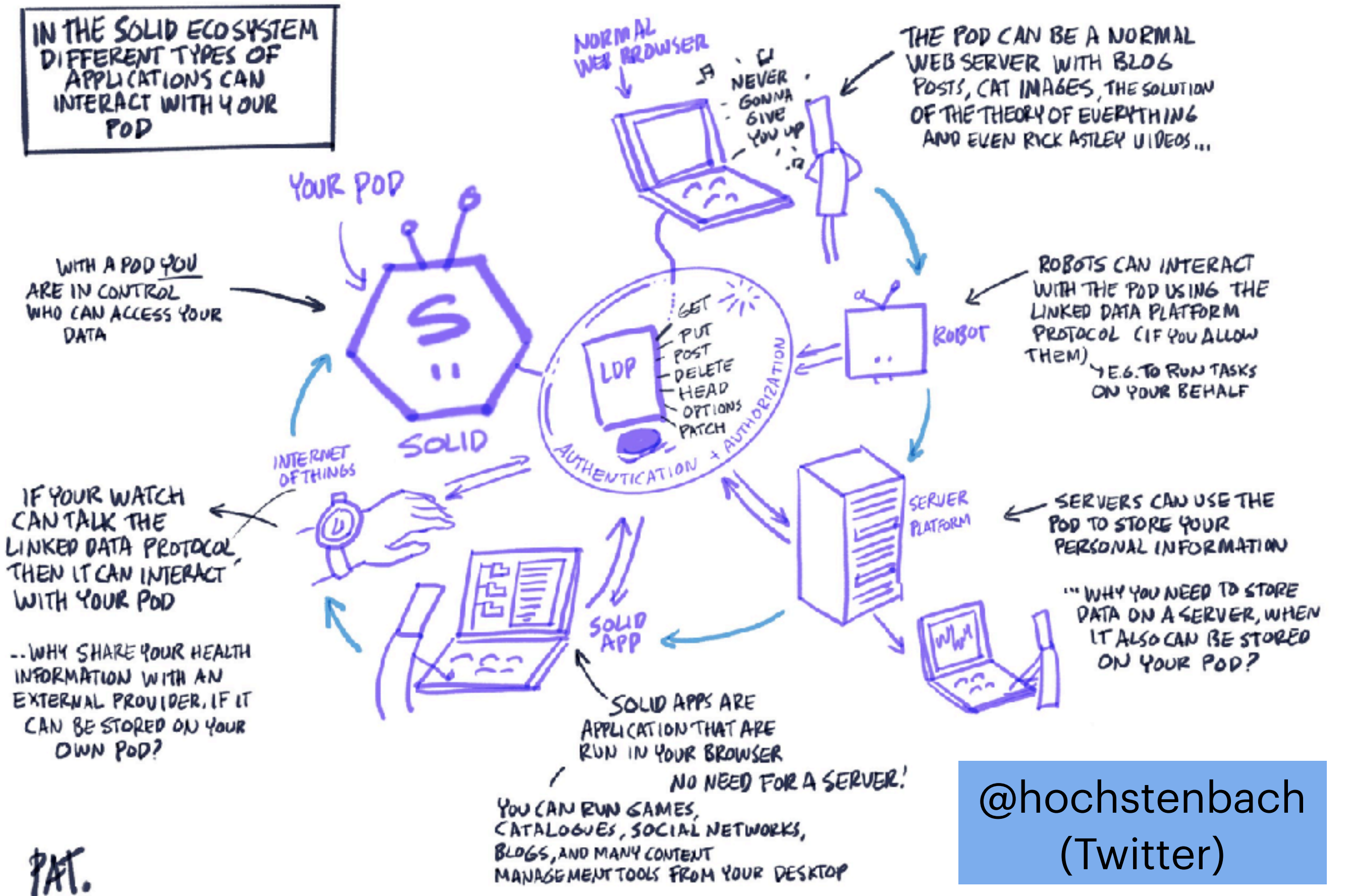
Decentralised

- You “control” where your data is stored
- You “control” how it is used by apps/services
- You offer choices and controls

What will SOLID need to work?

- A new way to express privacy and preferences
- User-friendly UI/UX *without dark patterns*
- Legal enforcement to make companies respect negotiation of user preferences and settings

SOLVEMBER #7 WHAT IS SOLID?



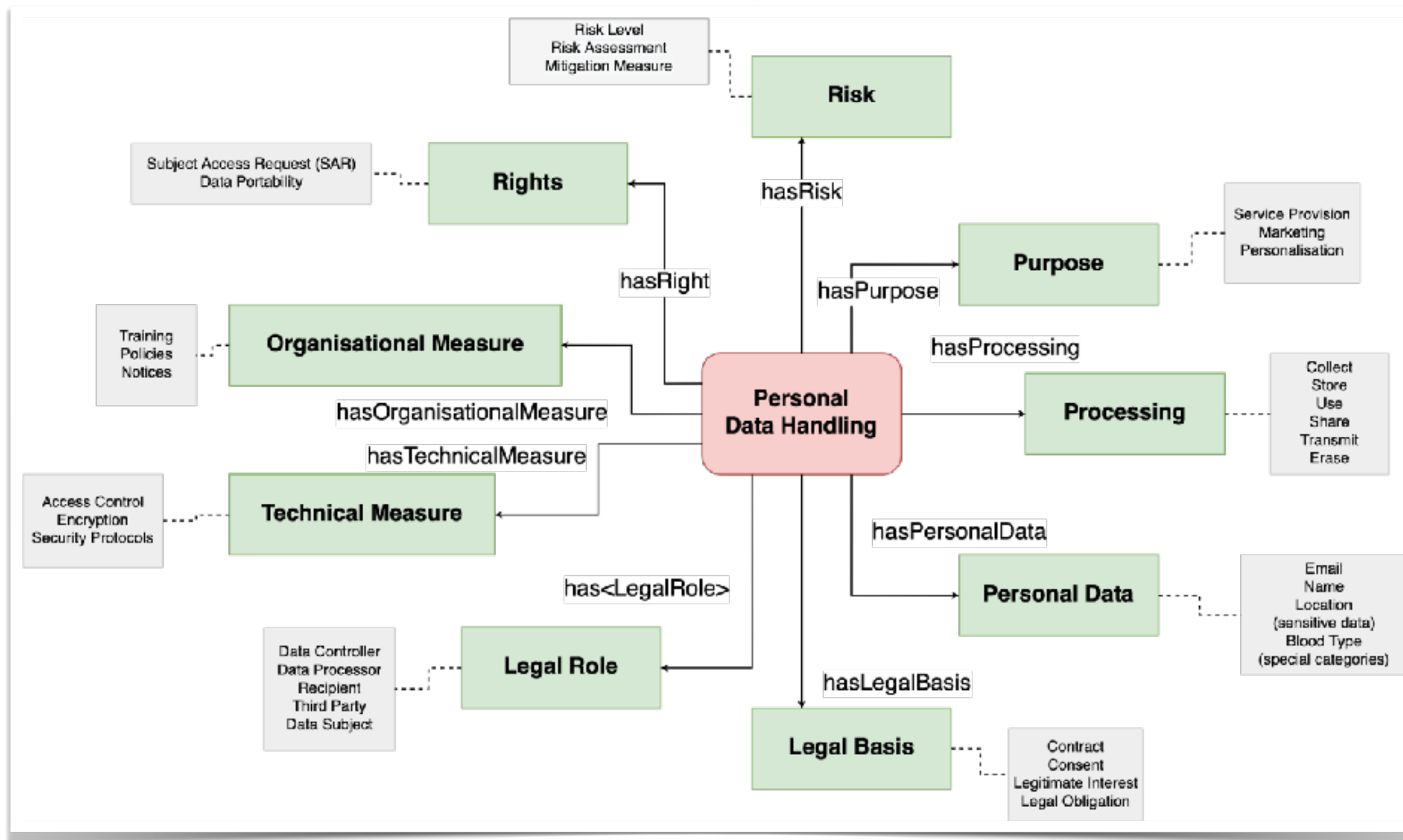
@hochstenbach
(Twitter)

What am I working on?

Privacy Risks, GDPR, Legal Compliance, Semantics

Machine-Readable Metadata for Automated Approaches

Data Privacy Vocabulary (DPV), v1 RC, 2022 <https://w3id.org/dpv>



DPV's taxonomies provide semantic interoperability, which enables new, innovative, smart, and automated solutions

Demonstrated usefulness for important use-cases, e.g. ROPA, consent, compliance checking

We're looking to the future! DGA / ePR / AI-Act / Data Spaces

The Data Privacy Vocabulary (DPV) reflects ~5 years of efforts in creating an open resource providing concepts related to personal data processing, privacy, data protection, and GDPR

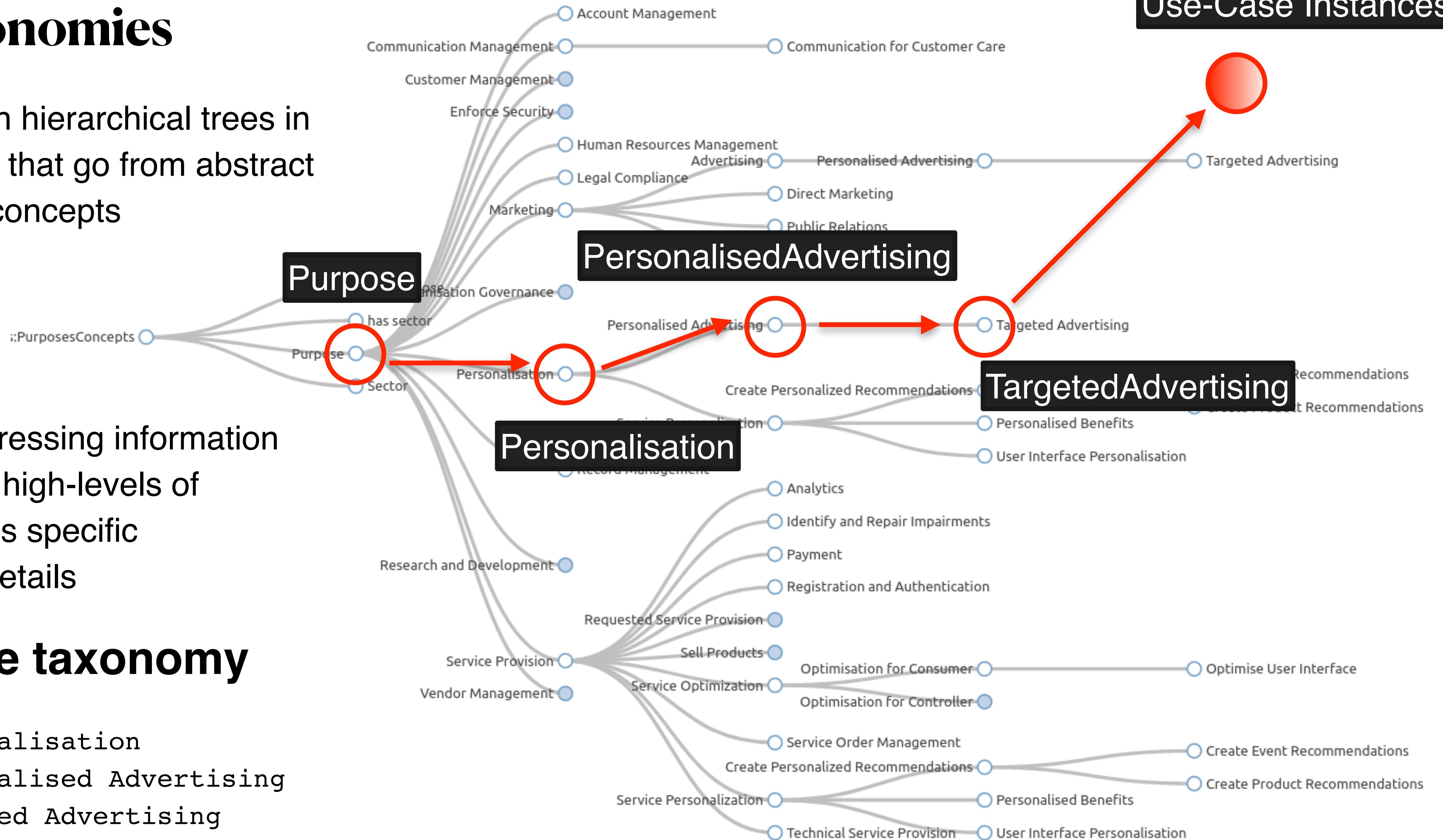
DPV Taxonomies

DPV provides rich hierarchical trees in top-down fashion that go from abstract to more specific concepts

This enables expressing information and rules at both high-levels of abstraction and as specific implementation details

E.g. Purpose taxonomy

Purpose → Personalisation
→ Personalised Advertising
→ Targeted Advertising



DPV Applications

current work

1. Register of Processing Activities (ROPA)
2. Consent Records
3. Compliance Checking
4. Impact Assessments (PIA / DPIA)
5. Data Input/Output Assistance
6. Annotating code / documents
7. Expressing and Evaluating Rules

work in progress

1. Risk Management
2. Data Breach Records
3. Subject Access Request
4. Data Portability
5. Data Transfers
6. Privacy Policies
7. Standards & Guidelines

Real-World Use-Cases

Privacy Policy Analysis

<https://openscience.adaptcentre.ie/privacy-policy/personalise/demo/policy.html>

Information We Collect

There are **three** general categories of information we collect.

data collected from user

1.1 Information You Give to Us.

1.1.1 Information that is **necessary** for provision of services

legitimate interest

We ask for and collect the following personal information about you when you use our service. This information is necessary for the adequate performance of the contract between you and us and to allow us to comply with our legal obligations. Without it, we may not be able to provide you with all the requested services.

data category

data type

- **Account Information** When you **sign up for an account**, we require certain information such as your **first name**, **last name**, **email address**, and **date of birth**.
- **Profile and Listing Information** To use certain features, we may ask you to provide additional information, which may include your **id** address, **phone number**, and a **profile picture**.
- **Identity Verification Information** To help create and maintain a trusted environment, we may collect identity verification information (such as **images of your government issued ID**, **passport**, **national ID card**, or **driving license**, as permitted by applicable laws) or other **authentication information**.
- **Payment Information** To use certain features of the such as **booking**, we may require you to provide certain **financial information** (like your **bank account** or **credit card information**) in order to facilitate the **processing of payments**.

process

consent

1.1.2 Information you **choose** to give us

You may choose to provide us with additional personal information in order to obtain a better user experience. This additional information

hide legend

	data category
	data type
	process
	automated
	legal basis
	data source
	data retention
	processor
	third-party
	data-sharing
	consent
	rights
	location

How to Complaint Better?

Making it easier to report, investigate, document, and resolve issues online

<https://brianlunch.github.io/ConsentAnnotationToolSite/#/study/>

Screenshot 4 Screenshot 5 Screenshot 6

Select random area if unsure.

similar technologies as well as the options you have to

Choose a Document Template (Preview Below):

GDPR

Save Document

Click here when you are haved used the tool.

Annotations

Clear All

1

Choose the Domain you are familiar with:

Hci

List of possible Issues:

☒ Choices for consent are not symmetric

Additional Comments

Accept button is prominently styled ; is a dark pattern

- ☐ Nudging towards giving consent
- ☐ Interface blocks access
- ☐ Controls for preference are confusing
- ☐ Wording of information is not specific
- ☐ Disparity between expression of consent and withdrawal

This Cookie Notice explains how we use cookies and similar technologies as well as the options you have to control them.

Cookies on Reddit

We use cookies on our websites for a number of purposes, including analytics and performance, functionality, and advertising. [Learn more about Reddit's use of cookies](#)

GDPR violations by www.Reddit.com

This report highlights the violations of GDPR clauses found in the consent dialogue box on the website www.Reddit.com as of Wed, 14 Apr 2021 13:17:30 GMT.

1 - Hci- GDPR

Issue Name: Choices for consent are not symmetric

User Comments: Accept button is prominently styled ; is a dark pattern

• Law Name: Freely Given (R43, A4-11)

Law Description: consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. If there is no reject button an affirmative action to not consent cannot be made.

Click and drag to highlight problematic areas of the images. Select random area if unsure.

Screenshot 2

1 of 3

17/11/2021, 21:00

React App

<https://brianlunch.github.io/ConsentAnnotationToolSite/#/ConsentAnnot...>

Cookies

Advertising Cookies

ctly identify you, but it cause we respect your es of cookies. Click on settings. However, blocking some types of cookies may impact your

Consent, Privacy, and Other Annoyances on the Web

Harshvardhan J. Pandit | pandith@tcd.ie | @coolharsh55

What Is the Internet Doing to Me? | 22 November 2022 | Trinity College Dublin