

IAPP EUROPE DATA PROTECTION CONGRESS 2023

BE PART OF SOMETHING

BIGGER

BRUSSELS
* BELGIUM *

#DPC23

Privacy Engineering: Consent Workshop

Moderator: Dr John Selby

Facilitators: Tina Maisonneuve, Annelies Moens,
Shannon Douma, Dr Christoph Bausewein

Brussels - 14 November 2023



WELCOME AND INTRODUCTIONS



Dr John Selby



Tina
Maisonneuve



Annelies
Moens



Shannon
Douma



Dr Christoph
Bausewein



AGENDA OUTLINE

Welcome and Introductions	09:00-09:10
Session 1 - When is Consent Valid and When to Use It? What is Consent and Why Should It Be Your Last Resort: Tina Maisonneuve Applying Consent Theory to a Real-World Scenario: Annelies Moens	09:10-10:00
Session 2 - How Can Poorly-Engineered Privacy Consent Get Your Organisation Into Trouble? Lawyers & Engineers Failing to Get Along: Shannon Douma Sensitive Information Creates Challenges: Dr Christoph Bausewein Case Study of Connected Vehicles and Fitbit: Annelies Moens Long-Term Costs to an Organisation of Poorly Managing Consent: Tina Maisonneuve	10:00-11:00
Break	11:00-11:15
Session 3 - Best Practices - How to Effectively Engineer Privacy Consent How to make a consent an <i>informed</i> consent: Dr Christoph Bausewein How Lawyers and Engineers can Centralize Consent: Shannon Douma	11:15-12:20
Closing Remarks	12:20-12:30



Session 1

When is Consent Valid and When to Use It?



What is consent & why should it be used as a last resort?



What is consent?

- Acceptable consent varies depending on geographical location.
- The General Data Protection Regulations (“GDPR”) requires consent to be
 - Freely given
 - Specific
 - Informed
 - Unambiguous indication of wishes



2. What does this mean in practice?

“Freely Given” means



No Imbalance of power Real choice and control for data subjects,
Unconditional Not tying performance of a contract to consent so can deliver a service without consent,
Granularity Freedom to choose which purposes they accept,
No Detriment Able to withdraw consent without detriment



Imbalance of power No choice,
Conditional Compelled to consent or will endure negative consequences,
General Consent bundled up as a non negotiable part of terms and conditions,
Detriment Unable to refuse or withdraw consent without detriment



“Specific” means?



Purpose specification Statement of a specific explicit and legitimate purpose for the intended processing activity

Granularity in consent Provide an opt in for each purpose

Separation of Information Provide specific information for each separate consent



General Purpose Broad statement of purpose of the intended processing activity inviting widening or blurring of purposes

Broad consent One opt in for many purposes

General Information. General information for different consents



“informed” means?



Transparency

- i. controller’s identity,
- ii. the purpose of each of the processing operations for which consent is sought,
- iii. what (type of) data will be collected and used,
- iv. the existence of the right to withdraw consent,
- v. information about the use of the data for automated decision-making in accordance with Article 22 (2)(c)36 where relevant, and vi. on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.3

Effective Delivery. Use of clear and plain language, presentation suitable to audience (written, oral audio or video), use of layering etc



Lack of transparency

Lack of Effective Delivery. Information not easily accessible i.e. relevant information in an obscure place, long privacy notices understand, use of legal jargon, excessive use of “may” etc



“unambiguous indication of wishes” means?



Action Deliberate action to consent



No Action Pre-ticked opt-in box /
opt-out constructions that require an
intervention from the data subject to
prevent agreement,
Silence or inactivity on the part of
the data subject,
Merely proceeding with a service.



What are the difficulties with consent?

1. Consent requirements
2. Consent fatigue
3. Demonstrating Compliance
4. Changing Consent
5. Cross Border Complexity
6. Age related consent
7. Cookie consent challenges



Applying Consent Theory to a Real-World Scenario



Applying Consent Theory to a Real-World Scenario

Case study removed from web version. Please contact [operations\[at\]privcore.com](mailto:operations@privcore.com)
if interested in the case study.



Consent risk checklist

1. Do you have a privacy notice to inform purpose and processing of personal information? Does it provide enough information?
2. Are you asking for consent where it is not required?
3. If relying on consent, are you going to use opt-in or opt-out consent or are you going to try to do better?
4. Are you asking the right people to consent? Does the person have capacity to consent?
5. Are you giving people a choice – if they don't consent what are the other options?
6. Is your consent clear, contained and stand alone?
7. What is the validity period of the consent? Can it be withdrawn?



Session 2

How Can Poorly-Engineered Consent
Get Your Organisation
Into Trouble?



When Privacy Engineers & Lawyers Don't Work Together



Consider this Scenario....

A Digital Advertising company is advised by Legal Counsel that customers must be provided with the option to Opt-Out of tracking when they are browsing on any websites associated with their services.

To address the Requirement, the Company's website engineer configures a Button on each website that Customers can click to opt-out. The Engineer also created "Fingerprinting" Technology so that even if a customer decided to opt-out the company could still gather insights through the user's browser functions.

Shortly after the Opt-Out button was moved to production the Company received a complaint from a Customer who believed that they had opted out of all tracking and believes that their information is still being collected without their consent.



What was wrong with the Engineer's Interpretation of the Opt-Out Requirement?



How could engaging a Privacy Engineer have helped in this situation?



A Privacy Engineer Can Solve the Language Barrier



Consent as a legal basis - Practical issues



This section removed from web version. Please contact [operations\[at\]privcore.com](mailto:operations@privcore.com) for more information.



Consent practices challenged

Recent examples of consent practices which are being challenged by privacy advocates



Connected cars example

* Privacy Not Included

moz://a

Product Reviews * Articles About

All Reviews

Best Of

Cars

Mental Health Apps

Entertainment

Smart Home

Wearables

Reproducti



📘 It's Official: Cars Are the Worst
🐦 Product Category We Have Ever
✉ Reviewed for Privacy



By Jen Caltrider, Misha Rykov and Zoë MacDonald | Sept. 6, 2023



Tesla example

Tesla's opt-out consent for vehicle data sharing:

<https://www.tesla.com/legal/privacy#vehicle-data>

Opting out of vehicle data:

Connectivity and performance is a core part of all Tesla vehicles and why some customers choose Tesla, allowing for advanced features and an enhanced driving experience.

By default, Tesla provides this seamless experience while protecting your privacy.

However, if you no longer wish for us to collect vehicle data or any other data from your Tesla vehicle, please contact us to deactivate connectivity.



Tesla example

Please note, certain advanced features such as over-the-air updates, remote services, and interactivity with mobile applications and in-car features such as location search, Internet radio, voice commands, and web browser functionality rely on such connectivity.

If you choose to opt out of vehicle data collection (with the exception of in-car Data Sharing preferences), we will not be able to know or notify you of issues applicable to your vehicle in real time. This may result in your vehicle suffering from reduced functionality, serious damage, or inoperability.



Fitbit example




Fitbit example

- NOYB filed three complaints against Fitbit in Austria, the Netherlands and Italy on 31 August 2023
- NOYB alleges that Fitbit forces new users of its app to consent to data transfers outside the EU
- Further, NOYB alleges that Fitbit does not enable individuals to withdraw their consent, rather they have to completely delete their account to stop data transfers outside the EU
- Fitbit is apparently using consent to share all health data routinely



I agree to the transfer of my personal data to the United States and other countries with different data protection laws. [Learn more.](#) [Link to privacy policy]

13:15 📶 📶 88%

<  fitbit

Sign Up

First name
First Name

Last name
Family name

Email address
Your account email

Password
Enter your secure password

I agree to the Fitbit Terms of Service.
• [Terms of Service](#)
Please also read the Privacy Policy, including the Cookie Use statement.
• [Privacy Policy](#)
• [Cookie Use](#)

I agree to the transfer of my personal data to the United States and other countries with different data protection laws.

Keep me updated about Fitbit products, news, and promotions.

[Next](#)



Consent not valid

- Even if you could use consent, NOYB argues not valid consent because:
 - Not informed consent and risks of transferring to third countries not advised
 - Recipients and countries not listed
 - Consent not voluntary (you have to delete your account if you don't want transfers to take place)



Longer term costs to an organisation of poorly managing consent

This section removed from web version. Please contact operations@privcore.com for more information.



Session 3

Best Practices: How to Effectively Engineer Consent

This section removed from web version. Please contact [operations\[at\]privcore.com](mailto:operations@privcore.com) for more information.



Resource List

- Daniel Solove, “Murky Consent: An approach to the fictions of consent in privacy law”, 104 Boston University Law Review (forthcoming 2024), draft August 2023
- Stefaan G. Verhulst, Laura Sandor, Julia Stamm, [“The urgent need to reimagine data consent”](#), Stanford Social Innovation Review, July 2023
- Mozilla Foundation, Jen Caltrider, Misha Rykov, Zoe MacDonald, Mozilla Foundation, [“It’s official: Cars are the worst product category we have ever reviewed for privacy.”](#) 6 September 2023
- NOYB, [‘Your fitbit is useless, unless you consent to unlawful data sharing’](#), 31 August 2023
- ABLI - FPF, Convergence series, Status of consent for processing personal data in [Singapore](#) and [Thailand](#), August 2022



Resource List

<https://oipc.sk.ca/assets/best-practices-for-gathering-informed-consent.pdf>

<https://english.igj.nl/medicines/clinical-trials-gcp/rules-for-clinical-trials/informed-consent-procedure>

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2020_05_consent_en.pdf

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/#what3>

<https://www.enforcementtracker.com/>



Resource List

- **Case law**
- [Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal \(ANSPDCP\) \(Case C-61/19\)](#)
- [Greek DPA decision \(No 26/2019\)](#)
- [Greek case](#)
- **References**
- [edpb_guidelines_202005_consent_en.pdf \(europa.eu\)](#)
- [Consent | ICO](#)
- [How should we obtain, record and manage consent? | ICO.](#)
- [Murky Consent: An Approach to the Fictions of Consent in Privacy Law by Daniel J. Solove :: SSRN](#)
- [Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence \(mit.edu\)](#)

