



A privacy reminder from Google

To be consistent with data protection laws, we're asking you to take a moment to review key points of Google's Privacy Policy. This is not about a change we've made - it's just a chance to review the key points below. **Click "I agree" when you're ready to continue, or explore other options on this page.**

Privacy and Consent

CT5142 AI and Ethics, WK3

Would you rather...?



- ▶ A. Have a perfect “legal translator” that explains to you exactly what you are agreeing to regarding your data when using online services, and spend a minimum of 15 minutes a week using it?
- ▶ Or
- ▶ B. Get an extra app for free that you enjoy and spend the 15 minutes a week on using that app, but without really knowing what the implications of your online activities are?

Some information on privacy principles



The 8 principles of data protection

1 Fair and lawful	2 Specific for its purpose	3 Adequate to needs	4 Accurate, up to date
5 Not kept longer than needed	6 Take into account people's rights	7 Kept safe and secure	8 Not be transferred outside the EEA

General Data Protection Regulation (GDPR, 2018)

Principles:

1. fairness, lawfulness and transparency:
 - ▶ Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. purpose limitation:
 - ▶ Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
3. data minimisation:
 - ▶ Personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed
4. Accuracy:
 - ▶ Personal data must be accurate and, where necessary, kept up to date

General Data Protection Regulation (GDPR, 2018)

5. storage limitation:

- ▶ Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

6. integrity and confidentiality

- ▶ Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Accountability

- ▶ The controller shall be responsible for and be able to demonstrate compliance with these principles

5 principles of the US Code of Fair Information Practices (1973)



There must be no personal data record keeping systems whose very existence is secret



There must be a way for a person to find out what information about the person is in a record and how it is used



There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent



There must be a way for a person to correct or amend a record of identifiable information about the person



Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

OECD Privacy Framework (1980) (1)

Collection limitation principle: there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject

Data quality principle: personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes should be accurate, complete and kept up-to-date

Purpose specification principle: the purposes for which personal data are collected should be specified no later than at the time of data collections and the subsequent use limited to the fulfilment of those purposes ... and specified on each occasion of change of purpose

OECD Privacy Framework (1980) (2)



4. Use limitation principle: personal data should not be disclosed, made available or otherwise used for purposes other than those specified ... except with the consent of the data subject, or by the authority of law



5. Security safeguards principle: personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data



6. Openness principle: There should be a general policy of openness ... with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity ... of the data controller

OECD Privacy Framework (1980) (3)



7. Individual participation principle: Individuals should have the right (a) to obtain from a data controller ... confirmation of whether or not the data controller has data relating to them,



(b) have communicated to them i. within a reasonable time, ii. At a charge, if any, that is not excessive, iii. In a reasonable manner, and iv. In a form that is readily intelligible ... and to challenge data relating to them ... and have the data erased, rectified, completed or amended



8. accountability principle: a data controller should be accountable for complying with measures which give effect to the principles stated above



Informed consent: ethical considerations

GDPR TOONS



The notice and consent paradigm

Service users need to be alerted to the fact that personal information is being collected by means of providing a general statement on privacy, a privacy policy (notice)

The privacy policy outlines in some detail what data is being processed and for what purposes.

The consumer needs to agree to this policy before such information can be collected (consent)

Rationale for notice and consent

Core ethical value: **Autonomy**

Assumes a rational, competent and diligent consumer who takes care to investigate the consequences of their actions, weighs pros and cons carefully and makes a reasoned decision on that basis

Goal: doing justice to consumer autonomy and diversity of preferences (rather than requiring a single privacy standard for all, regardless of preferences)

Ethical responsibilities in informed consent

Informed consent as core ethical concepts in professional ethics, healthcare ethics and research ethics

Transactional concept, i.e. about interaction between professional/service provider and client/service user

Ethical acknowledgement of **asymmetry and power differential** between highly informed professional or provider and lay person who generally has less knowledge and power and is often dependent on the service provider

Ethical responsibility of professional or provider to **facilitate client in making a meaningful decision** (and not abuse powerful position)

Elements of Informed Consent (Beauchamp & Childress 2012)

A. Threshold elements:

- ▶ Competence / capacity:
The person who consents is not limited in their decision-making capacity and can make meaningful, thought-out decisions
- ▶ Voluntariness: the person who consents is not coerced, unduly pressured or inappropriately induced to consent

Elements of Informed Consent (Beauchamp & Childress 2012)

B. Information elements

- ▶ Information: the service provider provides selected relevant information that pertains to the decision whether to consent in an understandable format
- ▶ Understanding: the service provider ensures that the information provided was understood adequately by the person who consents

6 Elements of informed consent (Beauchamp & Childress 2012)

C. Consent elements

- ▶ Decision: based on the information provided during the process, the person who consents decides which option to choose
- ▶ Authorization: the person who consents authorizes the service provider to go ahead with the outlined interventions or practices

Standards of disclosure



Professional practice standard:
disclose what is generally
considered appropriate within
the profession

Benefit: experts best placed to
understand disclosure process and
clients' needs
Problem: self-interest, paternalism



Subjective standard: disclose
what the individual in question
wants to know

Benefit: adapts to individual needs
Problem: might not cover relevant
information if subject is not
interested or does not know what to
ask



Reasonable person standard:
disclose what an average
reasonable person would want
to know

Benefit: provides a normative
standard
Problem: who decides what is
reasonable?

Informed consent information in research



the purpose and objectives of the research project



what exactly participating in the research entails, in terms of concrete research activities to be performed and other practical requirements



any related costs or benefits arising from participation



any risks or harm, particular burdens or extensive time requirements related to participation; risks need to be identified in terms of their likelihood.



any potential benefits arising from research participation

Informed consent information in research



Concrete explanation of confidentiality and anonymity of information shared during research, data protection practices, and potential limits to confidentiality



Who to contact if a participant has concerns about the project, complaints, or experiences negative effects from participation.



State if a research ethics committee has given approval for a project, and include name, address and contact details for the committee.



Addressing challenges of consent

Typical challenges in informed consent



Person who consents frequently finds it difficult to understand provided information material



Material is often presented at an inappropriate reading level and/or includes specialist jargon (e.g. legalese)



Preexisting assumptions by users may be resistant to efforts at explanations



Not really trying to enable participant to make a meaningful decision

Problems with privacy notice and consent online



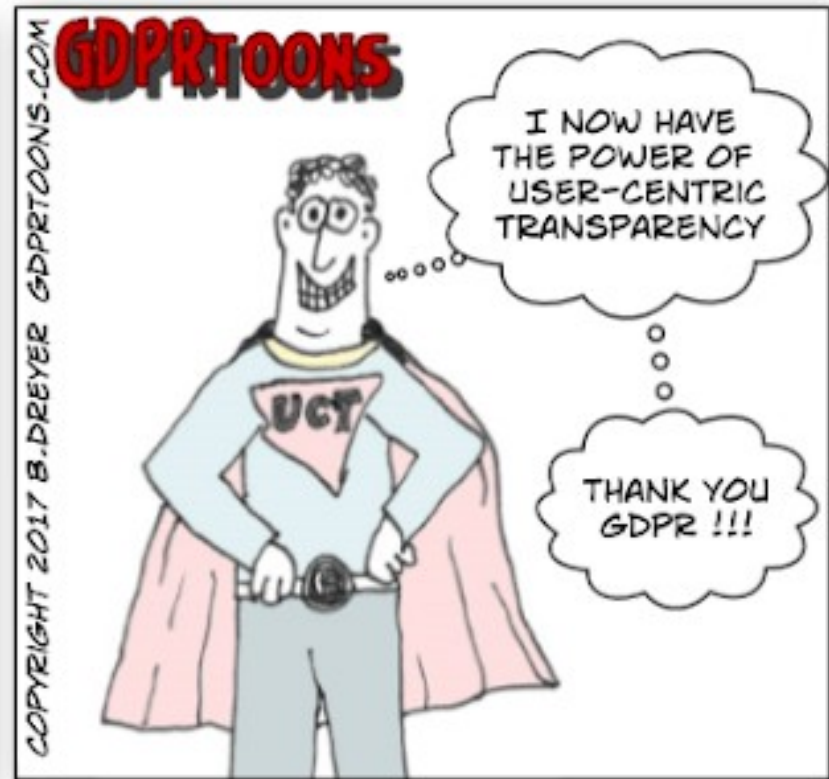
Service users rarely even read privacy statements, instead just “click through” (privacy paradox)



Potential misunderstanding: “privacy policy” taken as meaning that the policy consists in protecting privacy, rather than that it is a statement that outlines in what way privacy is being dealt with (i.e. potentially not very privacy respecting)



It is rational not to want to waste time reading privacy policies!



Calo on “visceral notice” as alternative



Deliver privacy notice not just verbally, but in a context-sensitive experiential format that *immediately and intuitively alerts user to privacy-relevant actions/practices*

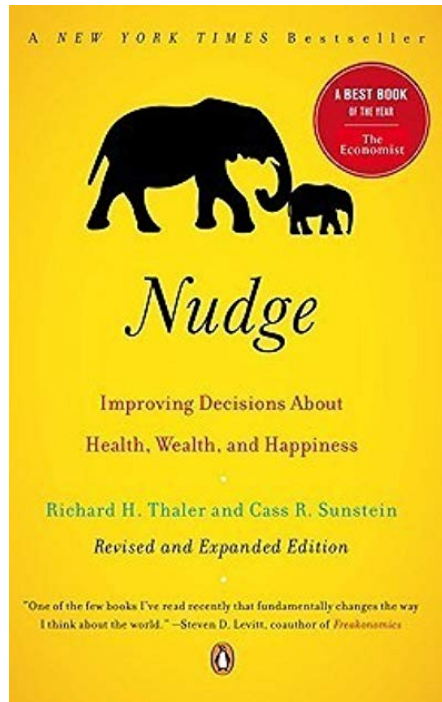


Leveraging a consumer’s experience of a product or service to warn or inform (e.g. shutter sounds)



Particularly suitable to online environment with multiple ways of providing online experiences

“Nudging”



- ▶ Nudging (Thaler & Sunstein 2008) focuses on leveraging “non-rational”, e.g. emotion-based mechanisms or framing effects, to achieve ethically desirable aims
 - ▶ E.g. by setting default setting to desirable aims
- ▶ “soft paternalism” or “liberal paternalism” which allows opting out for any interested, engaged user of those systems

Visceral notice & „nudging“

Visceral notice has some similarities, it also leverages psychological dispositions

But its main purpose is to make mechanisms transparent, rather than nudging users into a certain direction and shaping their preferences

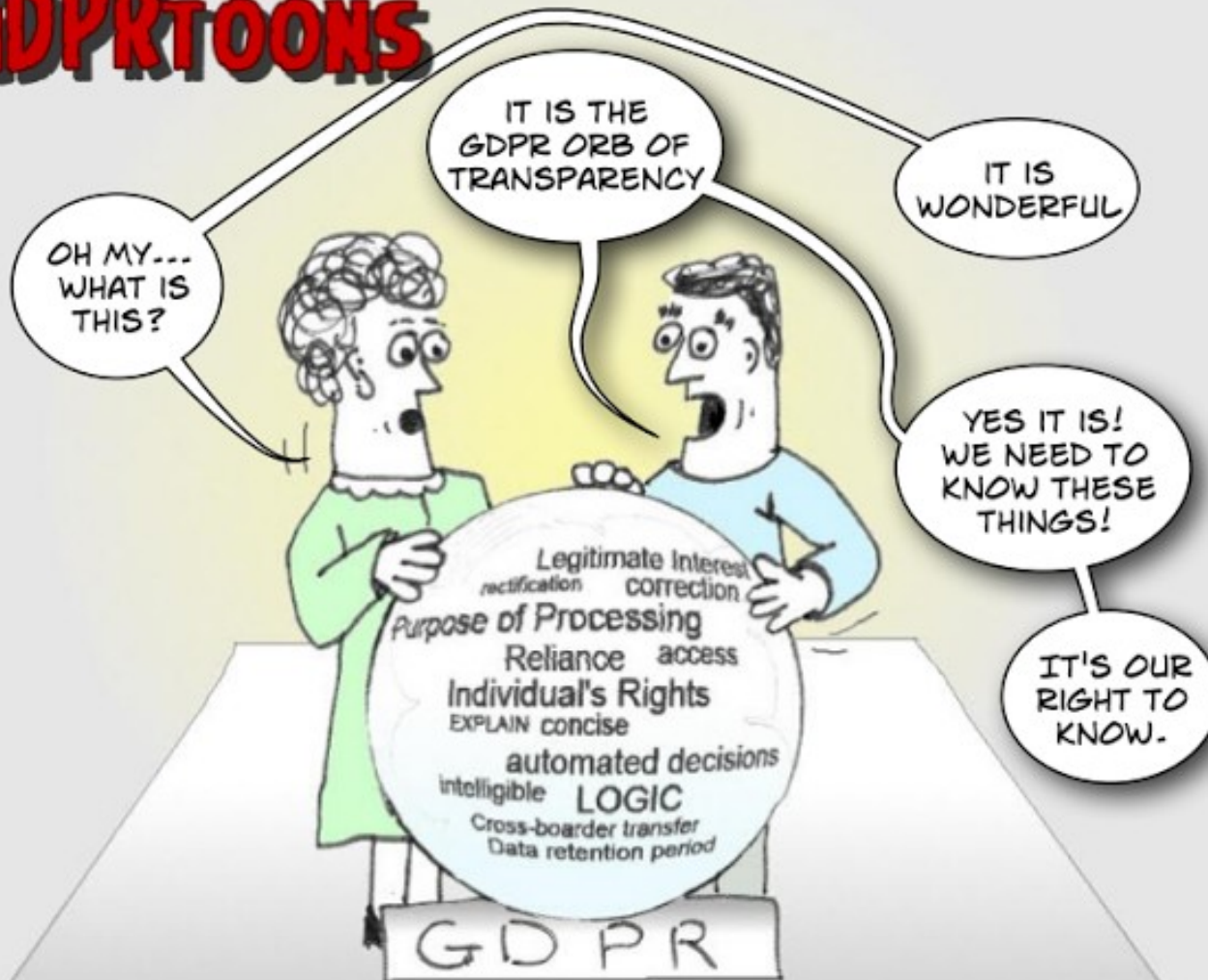


Consent, transparency and explainable AI

please
explain

GDPR TOONS

COPYRIGHT 2017 B.DREYER GDPRTOONS.COM



Transparency in GDPR

- ▶ personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject
- ▶ Prospective transparency:
 - ▶ individuals must be informed about the ongoing data processing before such processing takes place
 - ▶ the information must come in an intelligible and easily accessible form
 - ▶ Includes: information about themselves (who), the quantity and quality of processed data (how), the time(-frame) of the processing activities (when), the reason (why), and the purpose of processing (what for)
- ▶ Retrospective transparency:
 - ▶ the possibility to trace back how and why a particular decision was reached
 - ▶ “right to explanation”, meaningful information about the logic involved

Transparency and consent

Ethical requirements for transparency based on ethical criteria of consent:

- ▶ adapting information to user characteristics and needs
- ▶ avoiding implicitly coercive consent contexts,
- ▶ elucidating in a user-friendly, specific, and concrete way what the system is doing
- ▶ supporting users in achieving understanding and facilitating users' reflection process
- ▶ allowing them to make decisions that reflect their wishes and values



Human factors challenges for transparency

Different user groups have different levels of knowledge, different interests, and may use technology differently

Voice controlled AI cannot visually display transparency information, i.e. different mode of information provision may be needed with different psychological characteristics

General problems of information processing in transparency (Ben-Shahar & Schneider 2014)

- Risk: Strategic uses of transparency by companies that may not lead to higher levels of knowledge (Ananny & Crawford 2016)

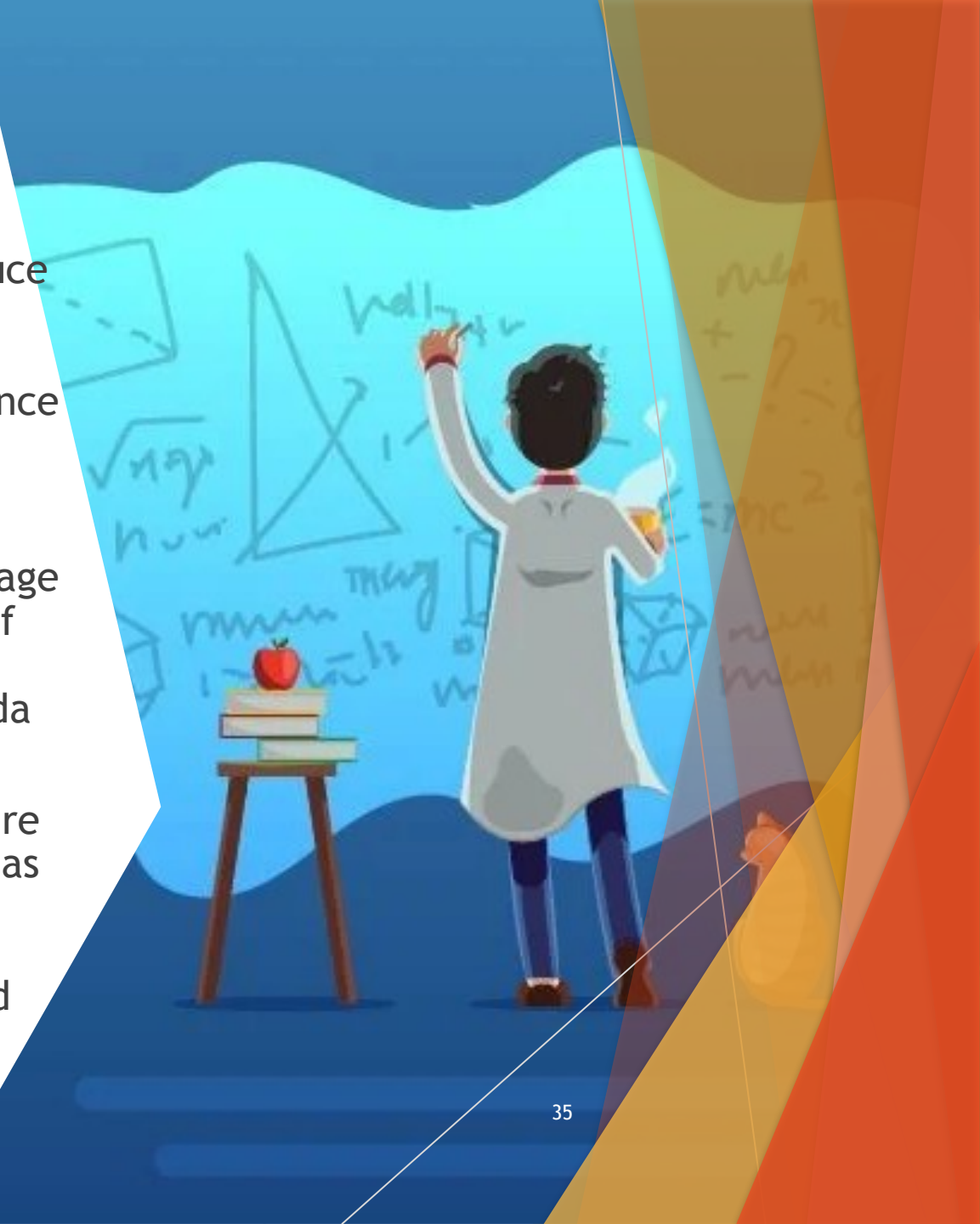
Multiple inconsistent effects of transparency on users shown in HCI, e.g. sometimes increasing trust, sometimes decreasing trust

Explainable AI (XAI)

- ▶ Functioning of AI often obscure („black box“)
- ▶ Difficulties in getting insight into exact functioning of Machine Learning algorithms
- ▶ XAI: efforts made in AI community to achieve explanation of AI system, in response to AI transparency and trust concerns

Goals of XAI

- ▶ DARPA: XAI aims to “produce more explainable models, while maintaining a high level of learning performance (prediction accuracy); and enable human users to understand, appropriately, trust, and effectively manage the emerging generation of artificially intelligent partners’ (Addadi & Berrada 2018)
- ▶ FAT: goal of XAI is “to ensure that algorithmic decisions as well as any data driving those decisions can be explained to end-users and other stakeholders in non-technical terms”



Function of XAI (Adadi & Berrada 2018)

- ▶ Explanation as basis of justification
- ▶ Explanation to better control and correct errors
- ▶ Explanation to improve
- ▶ Explanation to discover new knowledge

- ▶ Human knowledge as different to AI, but humans need to use and interact with AI, therefore “translation” is needed
- ▶ “Human-like” and “human-friendly” explanations