Introduction to Usable Privacy

Privacy Seminar 2026
26 February 2026
Christine Utz

AGENDA

- What is usable privacy?
- The human factor in privacy (& security)
- Challenges for usable privacy
- Usable privacy research
- Current topics

What is usable privacy?

WHAT IS USABLE PRIVACY?

Usability:

- Roughly: the ability of a system to allow its users to perform their tasks safely, effectively, and efficiently while enjoying the experience
- Focus on the **human factor**
- Multitude of definitions and frameworks

Privacy:

- Multitude of definitions
- See slides from Lecture 1

Lee et al. via Wikipedia, https://en.wikipedia.org/wiki/Usability#cite_note-1

The human factor in privacy (& security)

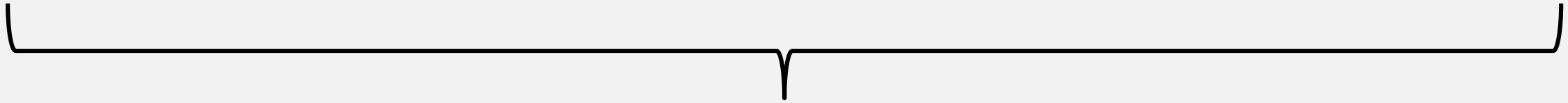
USERS ARE NOT MACHINES

End users:

- Top priority: functionality & convenience
- Security & privacy only secondary goals
- May be tired, stressed, or otherwise unattentive
- …

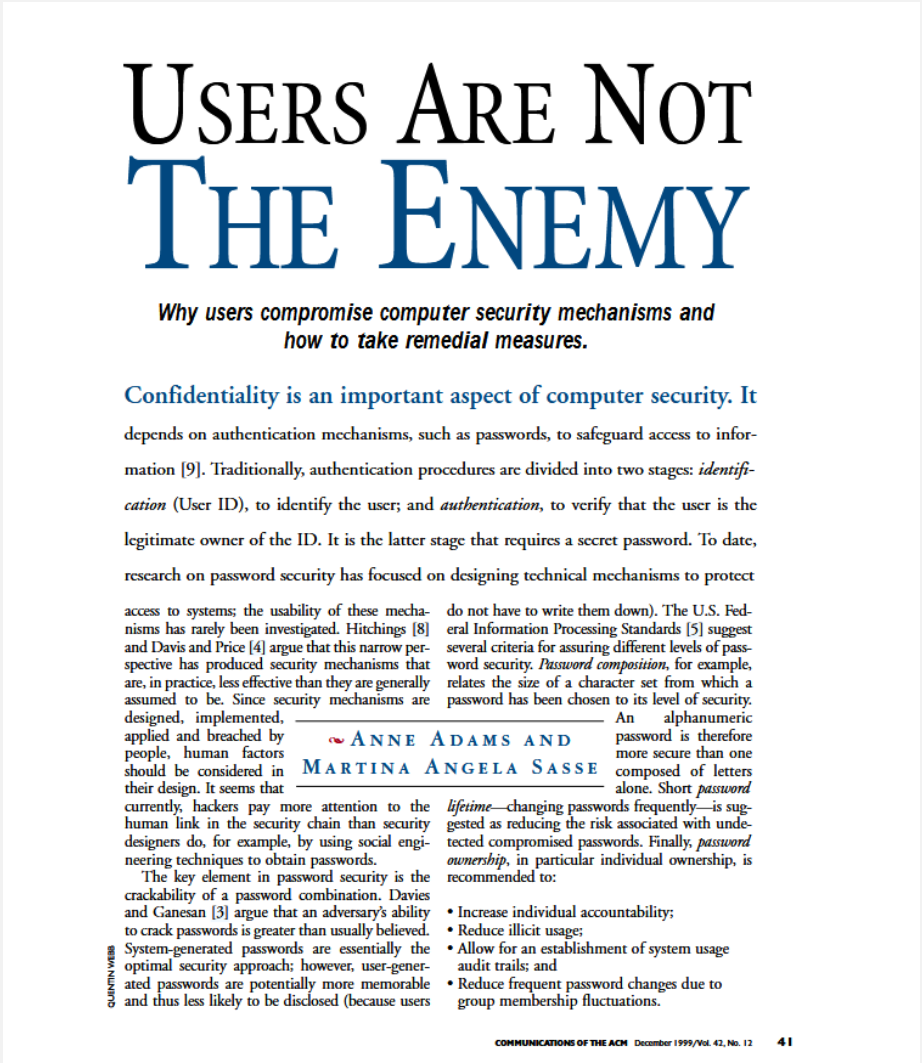
Developers:

- Top priorities: functionality & efficiency
- Security & privacy only secondary goals
- Typically operate under high pressure and resource constraints
- …



Work **with** human users and their flaws to design systems that are still private and secure.

WORK WITH, NOT AGAINST USERS



USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords.

The key element in password security is the crackability of a password combination. Davies and Ganesan [3] argue that an adversary's ability to crack passwords is greater than usually believed. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed (because users do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password lifetime*—changing passwords frequently—is suggested as reducing the risk associated with undetected compromised passwords. Finally, *password ownership*, in particular individual ownership, is recommended to:

- Increase individual accountability;
- Reduce illicit usage;
- Allow for an establishment of system usage audit trails; and
- Reduce frequent password changes due to group membership fluctuations.

ANNE ADAMS AND MARTINA ANGELA SASSE

QUENTIN WEBB

Developers Are Not the Enemy!

The Need for Usable Security APIs

Matthew Green | Johns Hopkins University
Matthew Smith | University of Bonn and Fraunhofer FKIE

Modern security practice has created an adversarial relationship between security software designers and developers. But developers aren't the enemy. To strengthen security systems across the board, security professionals must focus on creating developer-friendly and developer-centric approaches.

IT security mechanisms are failing to keep pace with the threats they face, increasingly exposing our systems and critical infrastructures to attacks. These failures are wide ranging and affect home users, enterprises, and governments alike. A 2014 study conducted by McAfee, Intel, and the Center for Strategic and International Studies estimates cybercrime's global cost to be US$400 billion per year.[1] The reasons for these failures can be classified broadly as either technical failures or human error.

For a long time, security research focused exclusively on the problem's technical side, viewing the human user as "the weakest link in the chain." However, the relatively new research domain of usable security and privacy takes a different stance: technology should adapt to its users rather than require users to adapt to technology. Three seminal papers—Mary Ellen Zurko and Richard Simon's "User-Centered Security,"[2] Anne Adams and M. Angela Sasse's "Users Are Not the Enemy,"[3] and Alma Whitten and J.D. Tygar's "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0"[4]—originated this school of thought. All argued that security experts shouldn't see users as problems to be dealt with; rather, they must communicate more with users and adopt user-centered design approaches.

The Developers' Role in Usable Security and Privacy

The usable security and privacy field studies end-user behavior, perceptions, problems, and wishes. Its researchers inform system administrators and software developers of the results and make concrete suggestions as to how developers and administrators can make their software and services more functional for end users. A classic example of usable security research is the study of users' password behavior, which has produced recommendations on how administrators should set policies that enable users to create strong yet memorable passwords.

There are many interesting, worthwhile research questions to be answered by studying end users. However, despite the earliest work in this domain calling for support for all involved actors—particularly developers[2]—current research almost entirely discounts the fact that administrators and software developers also make mistakes and need help as much, if not more, than end users (Ivan Flechais and his colleagues' work is one notable exception.[5]) Critically, whereas end users normally only endanger themselves, if administrators or developers make mistakes, they endanger all

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/16/$33.00 © 2016 IEEE

- Adams & Sasse, Communications of the ACM 42 (12), 1999, pp. 41–46, https://doi.org/10.1145/322796.322806
- Green & Smith, IEEE Security & Privacy 14 (5), 2016, pp. 40–46, https://doi.org/10.1109/MSP.2016.111

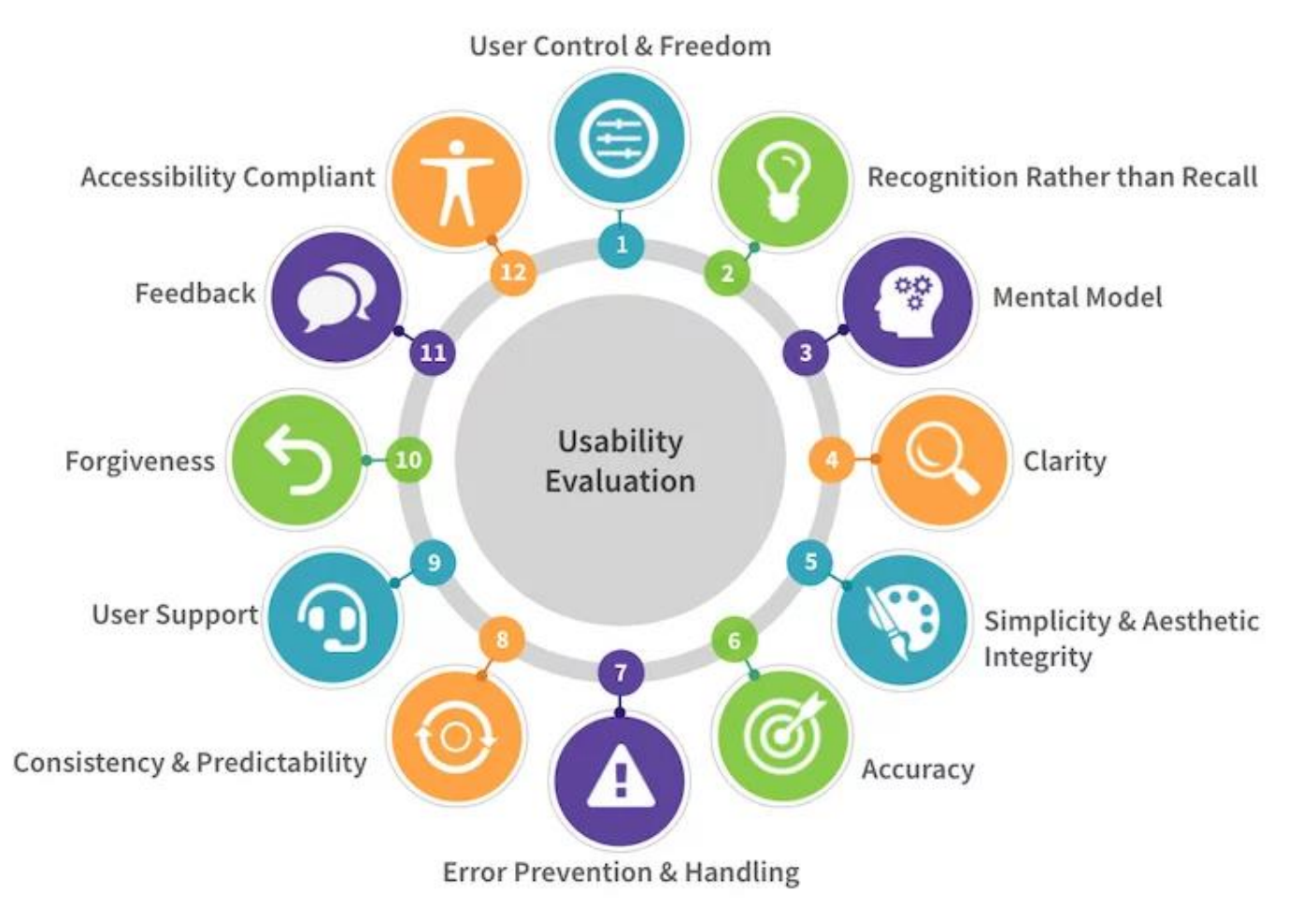
USABILITY PRINCIPLES

ISO Dialogue Principles (ISO 9241-110)

- Suitability for the user's tasks
- Self-descriptiveness
- Conformity with user expectations
- Learnability
- Controllability
- Robustness against user error
- User engagement

As reported by Rolf Molich, DialogDesign, https://www.dialogdesign.dk/isos-dialogue-principles-2019/

USABILITY PRINCIPLES



Stanford University Improvement, Analytics, and Innovation Services, https://improvement.stanford.edu/resources/usability-principles

USABLE SECURITY & PRIVACY

Security vs. HCI vs. Usable Security

Security
What is the space of possible passwords? How can we make the password space larger to make the password harder to guess? How are the stored passwords secured? Can an **attacker** gain knowledge by observing a user entering her password?

TYPICAL QUESTIONS

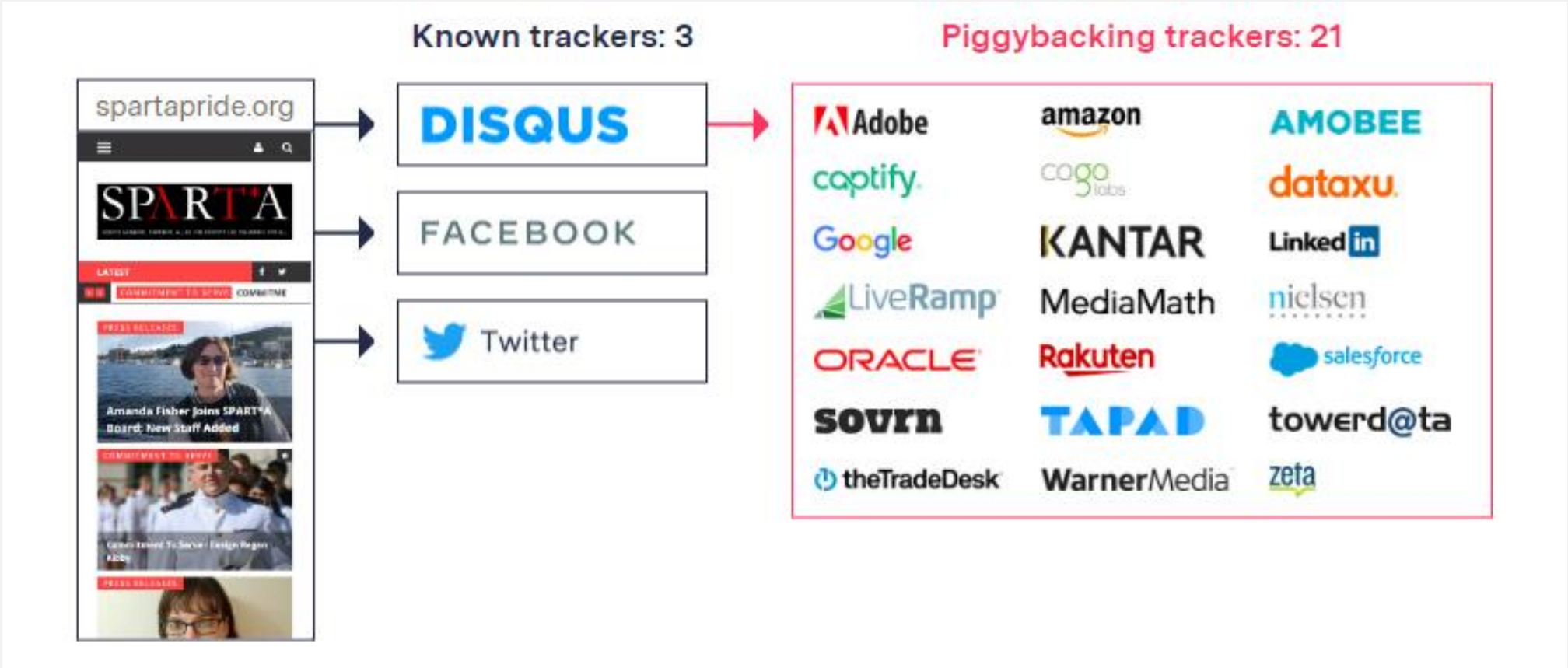
- How do non-technical people think about systems and associated privacy risks (**mental models**)?
- What **data** are users willing to disclose in which contexts?
- What could be done to **increase** this awareness?
- Do privacy perceptions **differ** between different demographics?
- Do users understand **privacy disclosures**?
- How do users perceive and interact with **privacy controls**?
- Are privacy options **transparently** shown or hidden on purpose?
- What **strategies** do users employ to protect their privacy online?
- Which **tradeoffs** are users willing to accept to protect their privacy?

Challenges for usable privacy

WHAT ARE CHALLENGES TO MAKE PRIVACY USABLE?

- Lack of awareness and knowledge
- “Notice & Consent” – overwhelming users with prompts and legalese
- Dark patterns and deceptive design
- Economics: business models
- Privacy – usability tradeoffs
- Interdependent privacy
- …

CHALLENGE: LACK OF KNOWLEDGE & AWARENESS



Aaron Sankin and Surya Mattu, The High Privacy Cost of a "Free" Website, https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites

NUDGES TO INCREASE AWARENESS

Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging

Hazim Almuhimedi,[1] Florian Schaub,[1] Norman Sadeh,[1]
Idris Adjerid,[2] Alessandro Acquisti,[1] Joshua Gluck,[1]
Lorrie Cranor,[1] Yuvraj Agarwal[1]

[1]Carnegie Mellon University
{hazim,fschaub,sadeh,acquisti,jgluck,
lorrie,yuvraj.agarwal}@cmu.edu

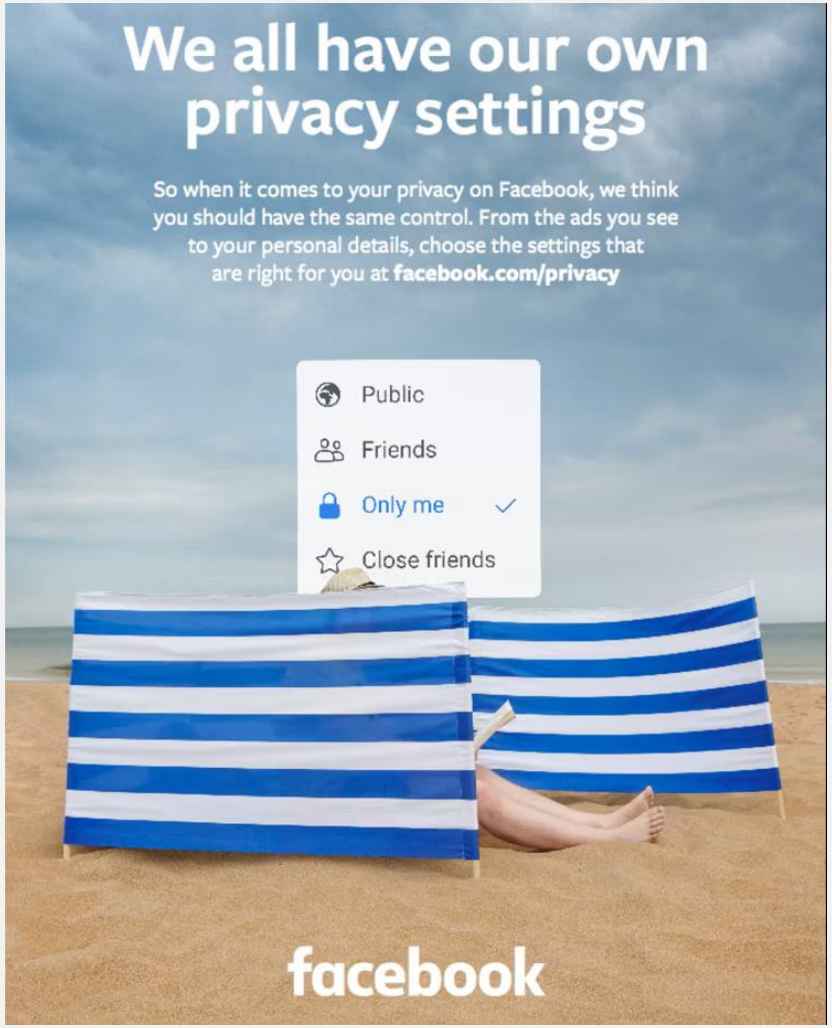
[2]University of Notre Dame
iadjerid@nd.edu

ABSTRACT

Smartphone users are often unaware of the data collected by apps running on their devices. We report on a study that evaluates the benefits of giving users an app permission manager and sending them nudges intended to raise their awareness of the data collected by their apps. Our study provides both qualitative and quantitative

biases, and decision heuristics that often lead to privacy-adverse decisions in favor of short-term benefits [3]. Privacy nudges have been proposed to support users in their privacy decision making [2]. Such nudges aim to make privacy risks more salient and help users move towards privacy settings that better align with their privacy expectations and concerns. One of the goals of

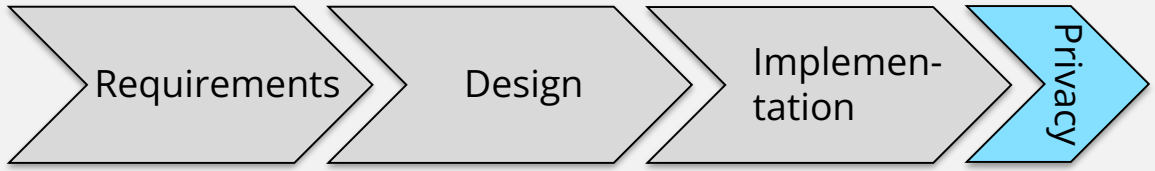
AWARENESS CAMPAIGNS



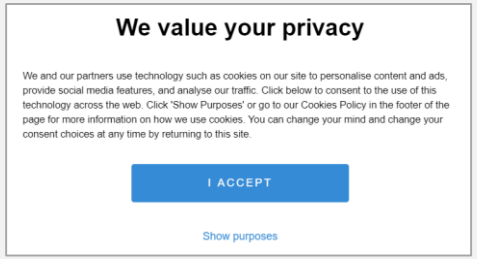
https://www.marketingweek.com/facebook-launches-uk-privacy-campaign/

CHALLENGE: “NOTICE AND CONSENT” APPROACH

“Notice and Consent“



…



PRIVACY POLICIES: LAW ...

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

… VS. REALITY

Art project by Dima Yarovinsky, https://www.designboom.com/readers/dima-yarovinsky-visualizes-facebook-instagram-snapchat-terms-of-service-05-07-2018/

CONSENT NOTICES: LAW …

Article 5(3) ePrivacy Directive (2002/58/EC)
(as of Directive 2009/136/EC)

5) Article 5(3) shall be replaced by the following:

'3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.';

governs the placement of information in users' browsers

Article 6(1)(a) GDPR

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

governs the processing of personal data

… VS. REALITY

Marktplaats

Marktplaats.nl gebruikt functionele, analytische en tracking cookies (en daarmee vergelijkbare technieken) om jouw ervaring op onze website te verbeteren en om je van relevante advertenties te voorzien.

Ook derde partijen kunnen cookies en vergelijkbare technieken plaatsen om jouw internetgedrag te volgen en je gepersonaliseerde advertenties te tonen binnen en/of buiten onze website.

Door op Cookies accepteren te klikken, ga je hiermee akkoord. Klik hier voor meer informatie

Cookies accepteren

Information storage and access

What this means: The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.

Depending on the type of data they collect, use, and process and other factors including privacy by design, certain partners rely on your consent while others require you to opt-out. For information on each vendor and to exercise your choices, see below. Or to opt-out, visit the NAI, DAA, or EDAA sites.

Allow All

1000mercis	Allow
1020, Inc. dba Placecast and Ericsson Emodo	Allow
1plusX AG	requires opt-out
2KDirect, Inc. (dba iPromote)	requires opt-out
33Across	Allow
7Hops.com Inc. (ZergNet)	requires opt-out
A Million Ads Limited	requires opt-out
A.Mob	Allow
Accorp Sp. z o.o.	requires opt-out
Active Agent AG	requires opt-out
Acuityads Inc.	Allow
ad6media	Allow
ADARA MEDIA UNLIMITED	Allow
AdClear GmbH	requires opt-out

cookie?

We use cookies to make your experience on this website better.

Yes please! No... I'm full

Evästeiden avulla parempia palveluja

Evästeiden avulla kerätyn tiedon ansiosta voimme tarjota sinulle parempia palveluja: käyttökokemus, sivustojen toiminta, sisältösuositukset ja mainonnan osuvuus paranevat. Evästeitä käytetään myös kävijämittaukseen.

Klikkaamalla ok hyväksyt, että Sanoma ja yhteistyökumppanit keräävät evästetietoa ja käyttävät sitä mainonnan ja markkinoinnin kohdentamiseen.

Lue lisää evästeistä ja hallinnoi omia asetuksiasi täällä.

OK

sanoma

Use of cookies:

Cookies are small data files that are sent from a website's server to your web browser, from where they are stored on your device.

All cookies | **Only essential cookies** | No cookies :(

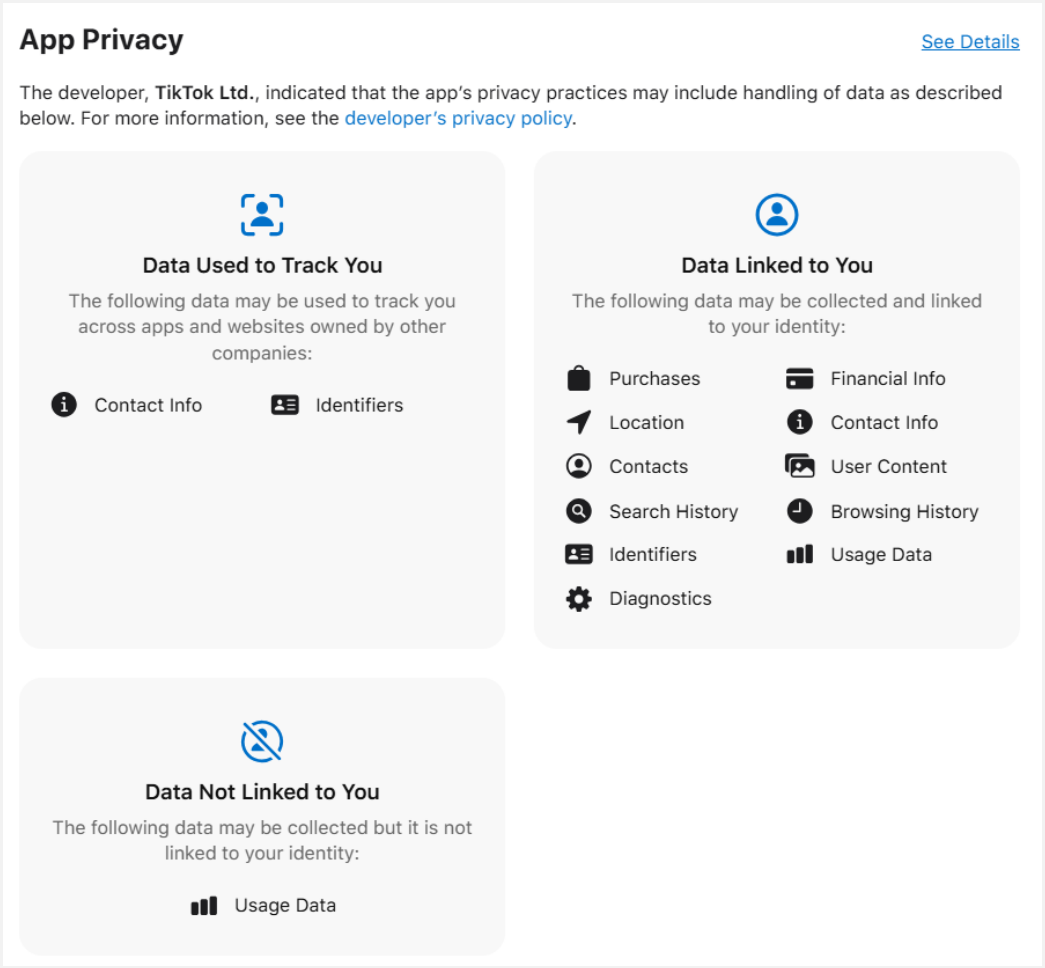
Essential cookies are used only to transmit the data online and are strictly necessary to make a website operational.

Cookies help us improve our web content and deliver a personalized experience. By using this website, you agree to our use of cookies.

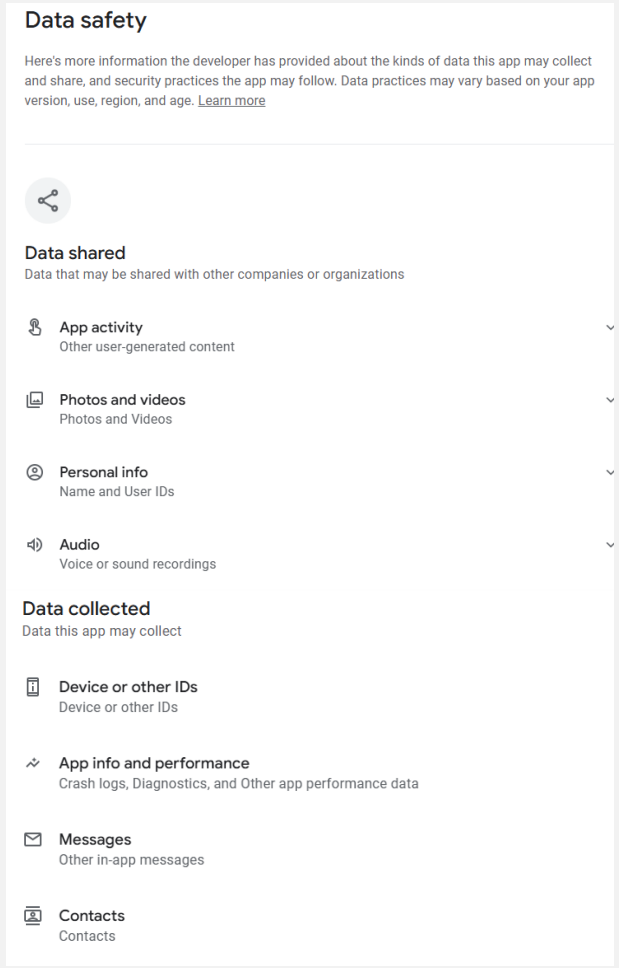
Type `man cookies` to learn more or `exit` to close.

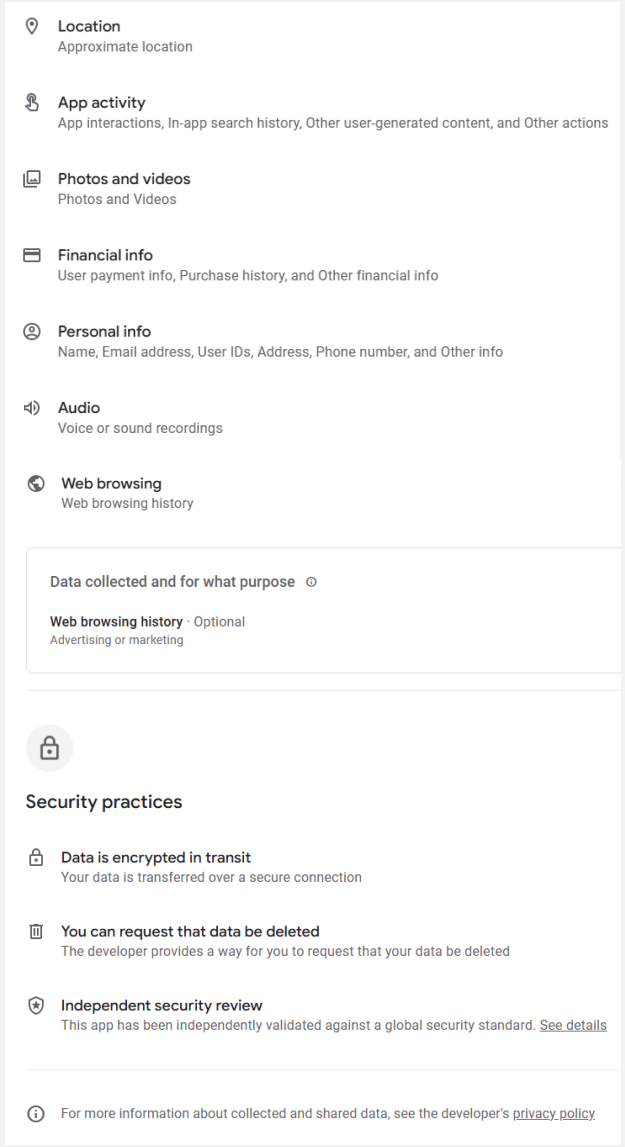
~ root#

PRIVACY “NUTRITION LABELS”



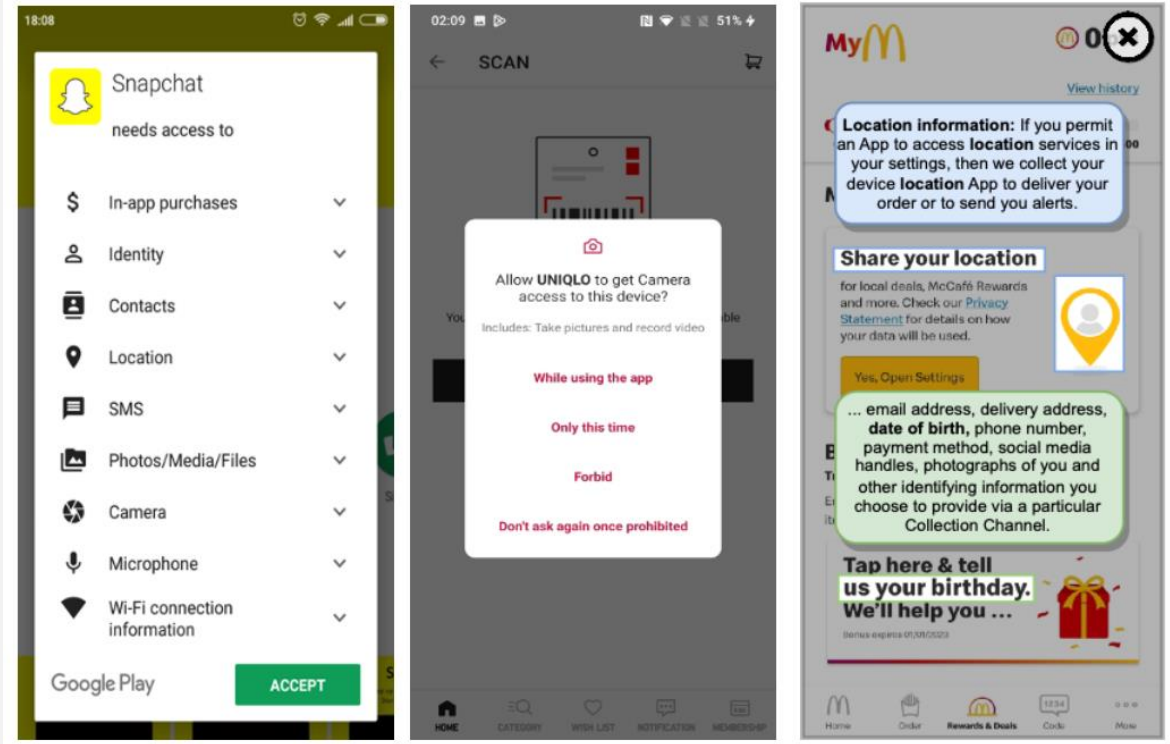
App Privacy Labels
(Apple App Store)





Data Safety Labels
(Google Play Store)

CONTEXTUALIZING PRIVACY INFORMATION



(a) Install-time (b) Invoke-time (c) Context-aware

Contextual privacy policy
(Pan et al., SeePrivacy)

The profile detailed how Carlson ridiculed his first-grade teacher in a book - and reported her shock on finding out.

Comments on Bailey's Instagram post were mostly appreciative, including clapping hand and beer emojis and sentiments including "American hero!!" and "Thank you!!"

His earlier posts included photos of a dog, hunting, fishing and other outdoor activities.

Allow Instagram content?

This article includes content provided by Instagram. We ask for your permission before anything is loaded, as they may be using cookies and other technologies. To view this content, **click 'Allow and continue'**.

✓ Allow and continue

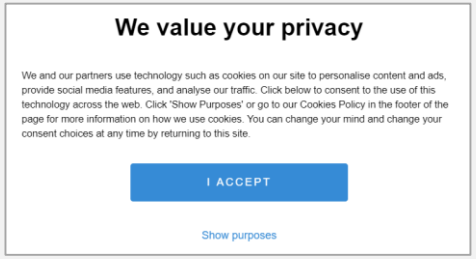
In a statement, Fox News said: "Ambushing Tucker Carlson while he is in a store with his family is totally inexcusable - no public figure should be accosted regardless of their political persuasion or beliefs simply due to the intolerance of another point of view."

Contextual consent button
(The Guardian)

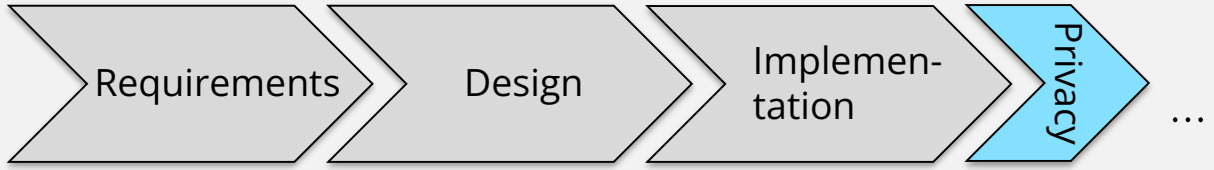
BROWSER-BASED PRIVACY CONTROLS

- **Do Not Track** (DNT) – failed due to lack of adoption
- **Global Privacy Control** (GPC) to send "Do Not Sell" requests under the CCPA, legally binding in California
- **Advanced Data Protection Control** (ADPC): designed for GDPR

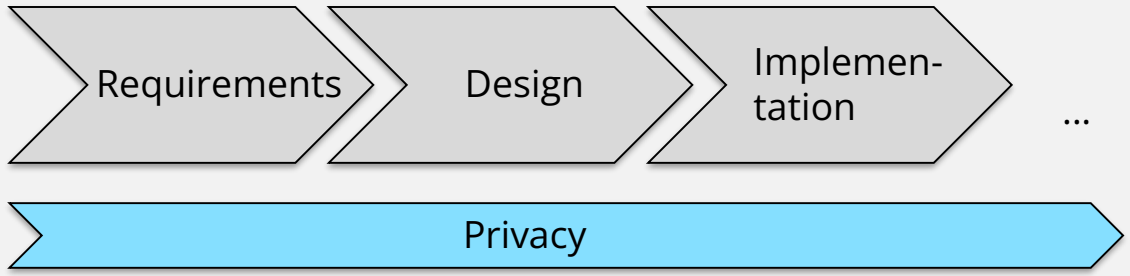
PRIVACY BY DESIGN



"Notice and Consent"



Privacy by Design



Article 25 GDPR
Data protection by design and by default

"2. The controller shall […] ensur[e] that, by default, **only personal data which are necessary** for each specific purpose of the processing are processed. That […] applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility."

CHALLENGE: DECEPTIVE (OR DARK) PATTERNS

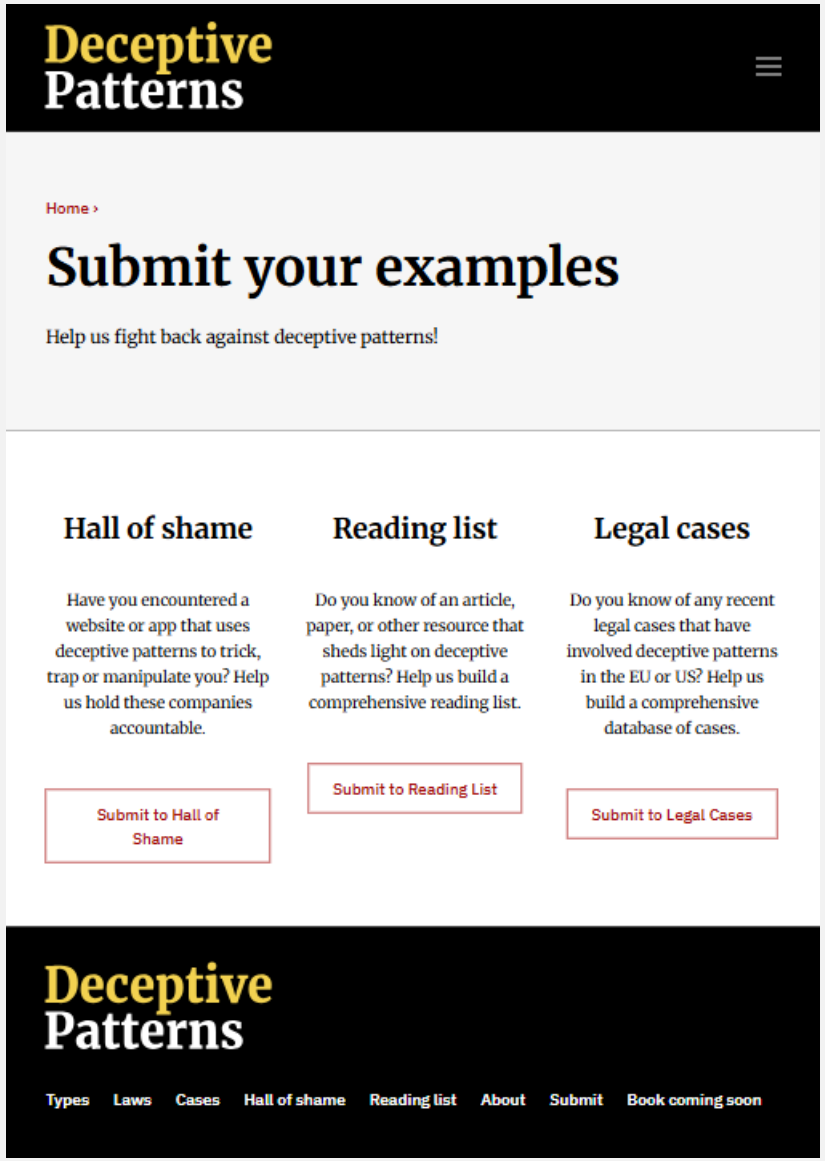
= user interfaces that have been carefully crafted to trick users into doing things [they would otherwise not have done] (Brignull 2011)

Dr. Harry Brignull
https://deceptive.design

Brignull, Dark Patterns: Deception vs. Honesty in UI Design, 2011, https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design/

TYPES

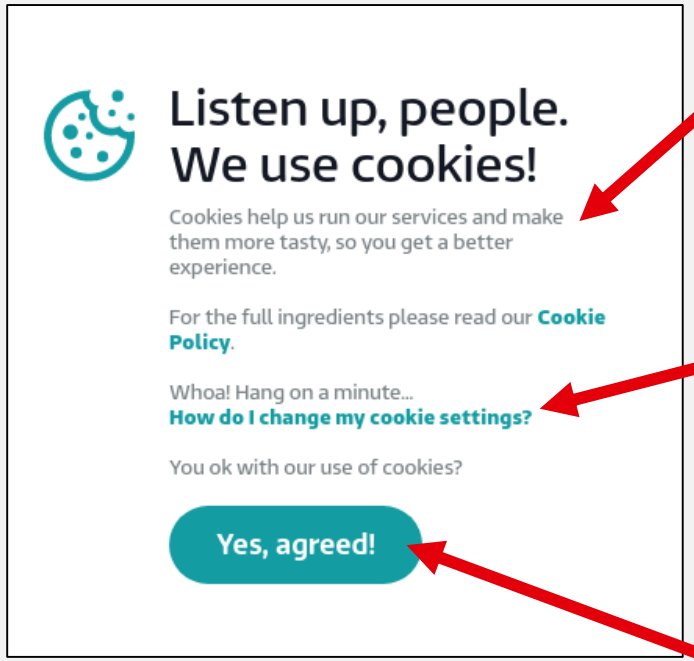
- Preselection
- Visual interference
- Trick wording
- Nagging
- Forced action
- Obstruction
- Confirmshaming
- Fake scarcity or urgency
- Hidden costs or subscription
- …



Taxonomy from https://deceptive.design (Brignull et al.)

EXAMPLE: CONSENT NOTICES

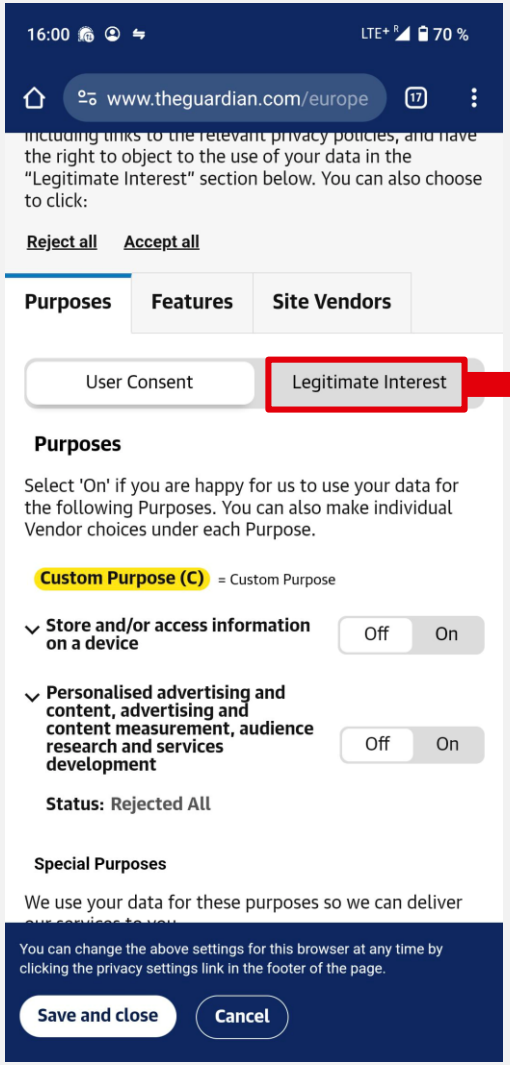
Consent: "**freely given**, specific, informed and unambiguous"

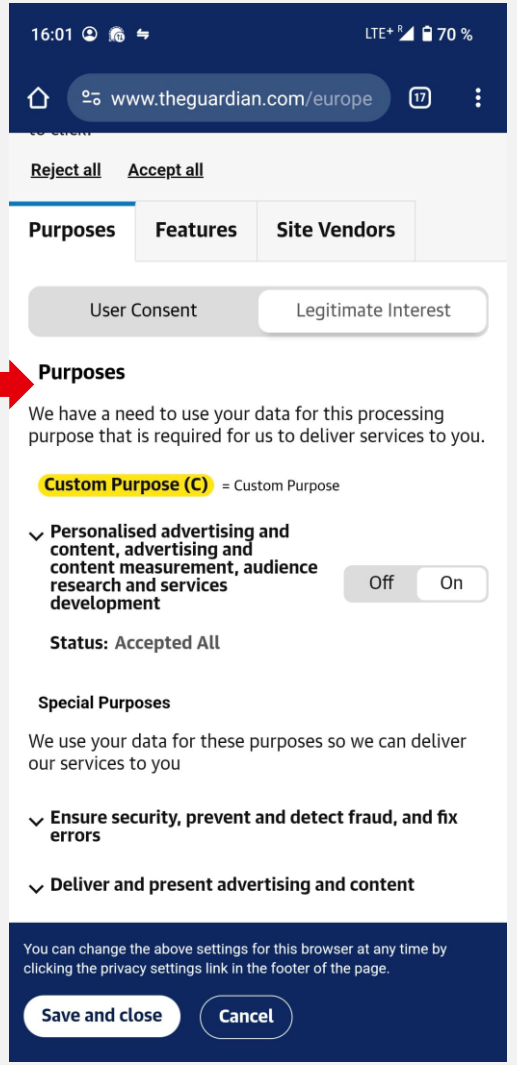


Only benefits of cookie use mentioned

"Decline" options hidden on second layer

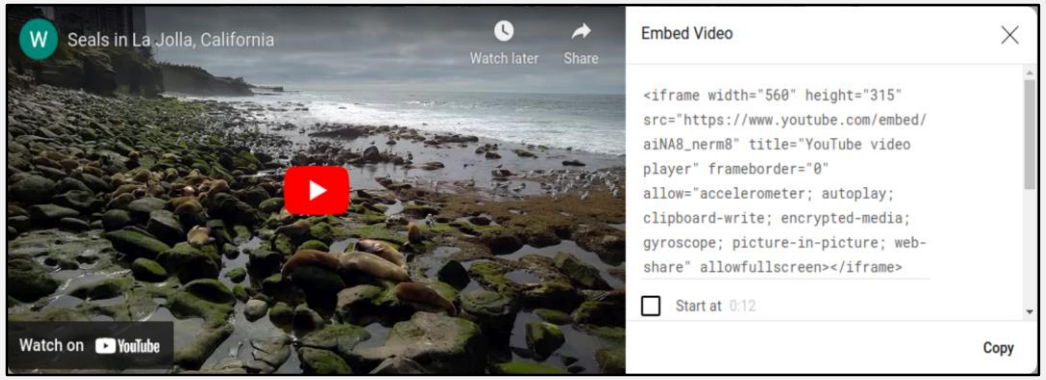
"Agree" button highlighted



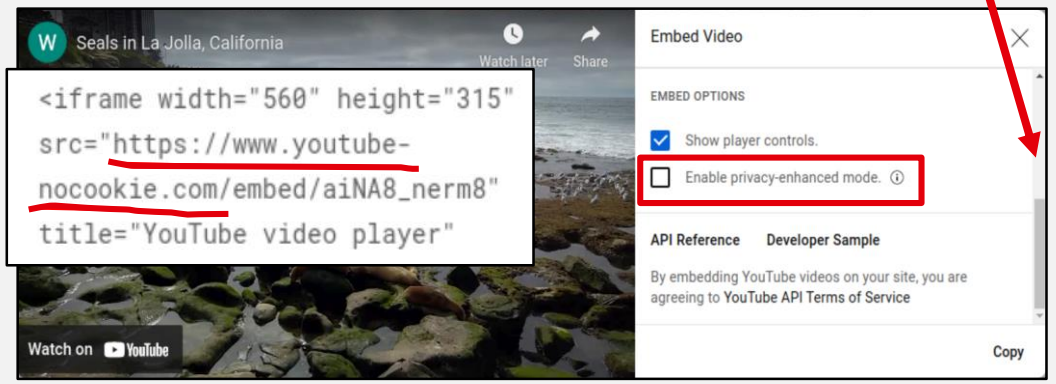


EXAMPLE: YOUTUBE

dark pattern: option only visible after scrolling down

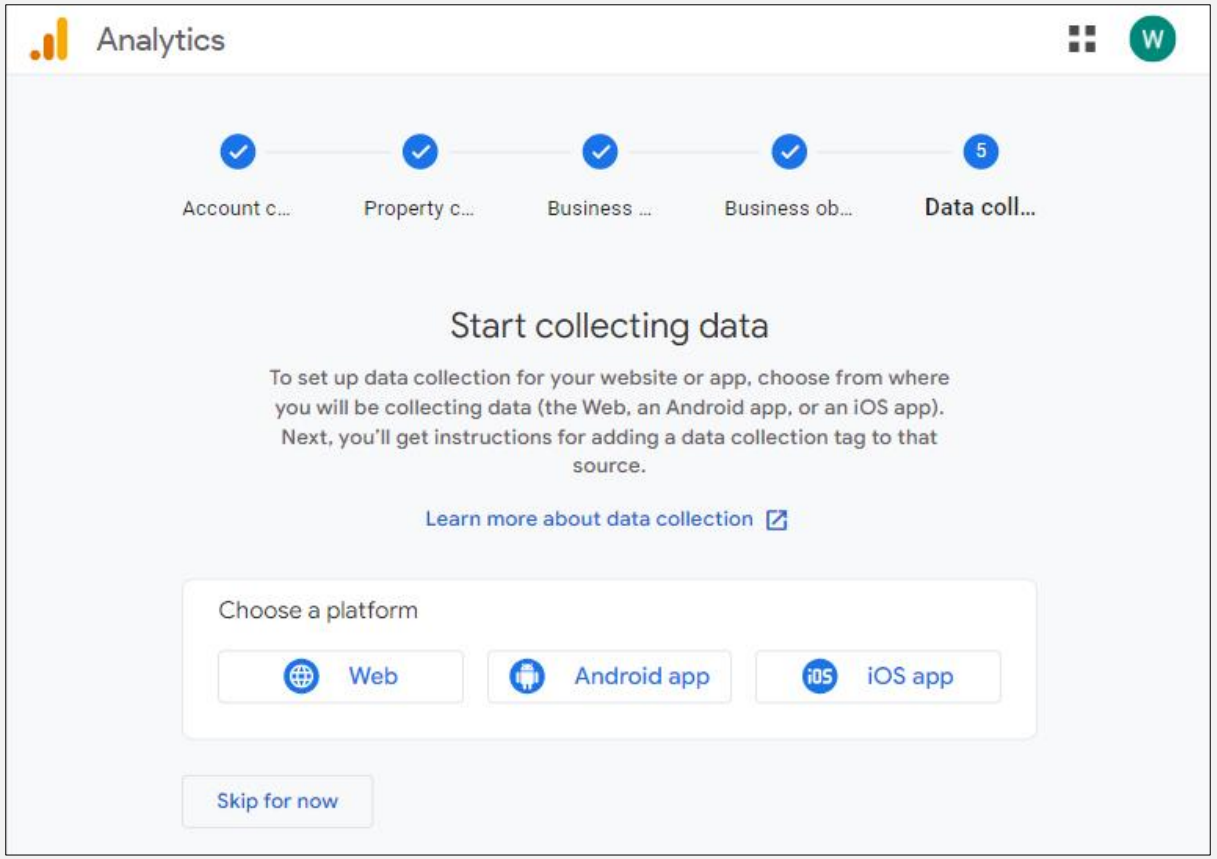


Default YouTube embed code: cookie set as soon as the website embedding the video is visited

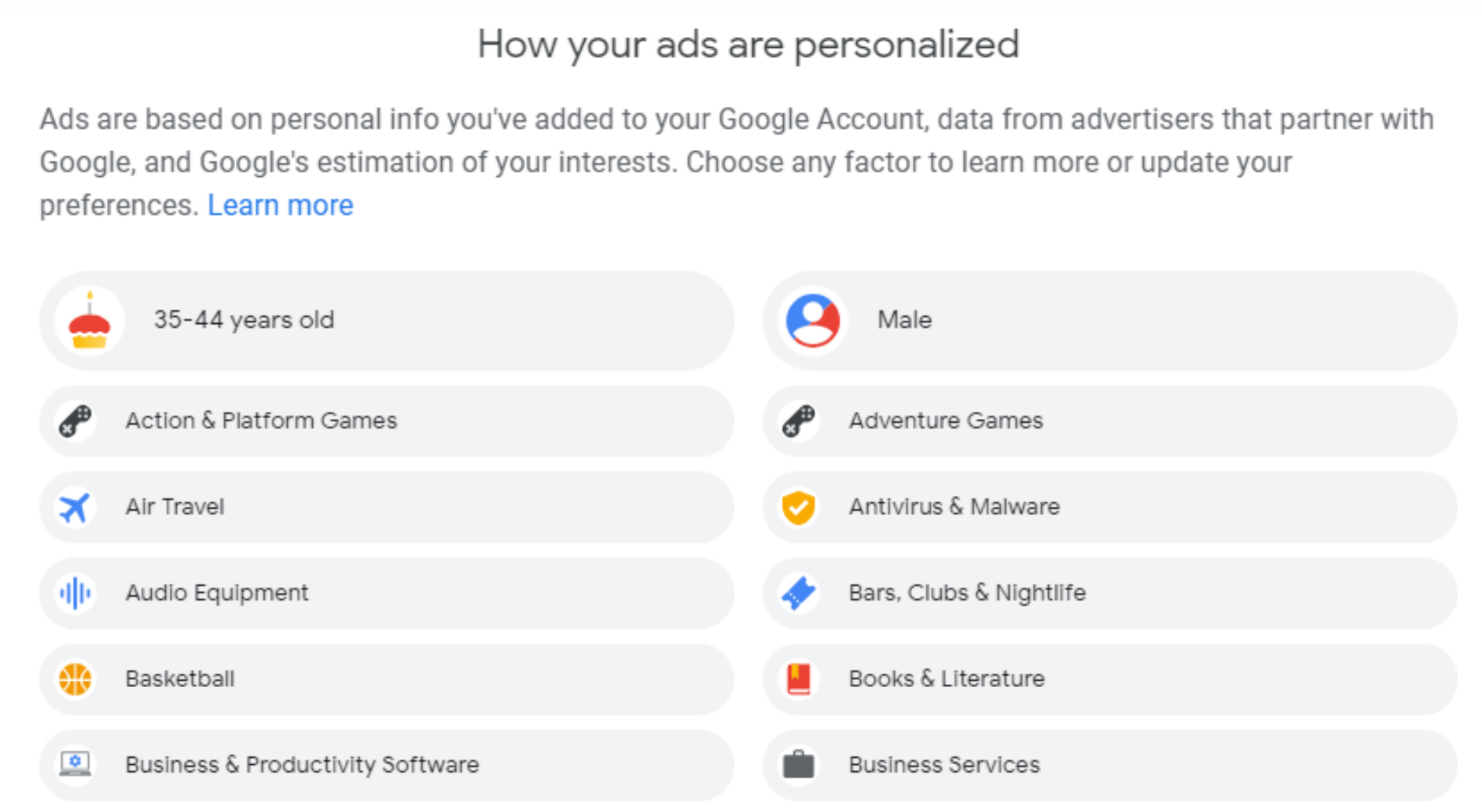


“Privacy-enhanced mode“: cookie only set upon interaction with the embedded video

ACTIVITY: DARK PATTERNS IN GOOGLE ANALYTICS

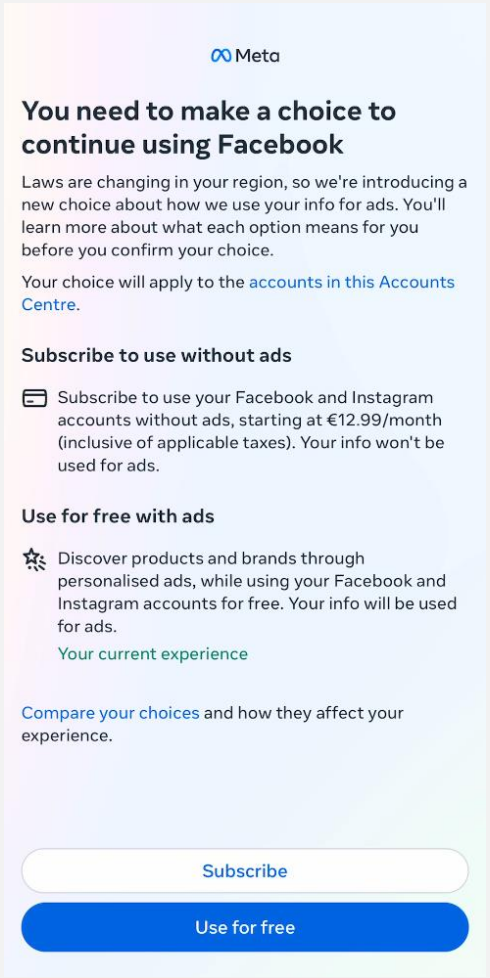


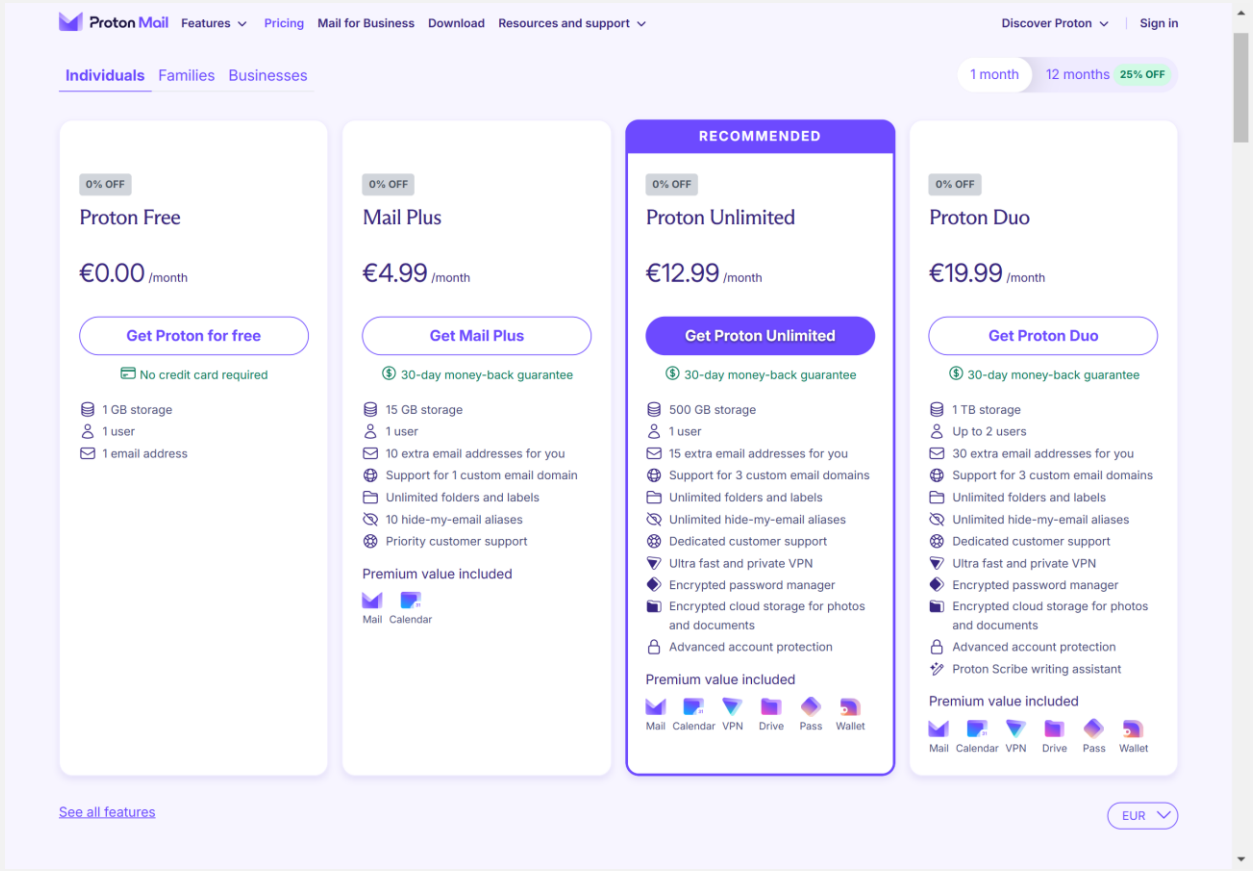
CHALLENGE: CONFLICTING BUSINESS INTERESTS



https://www.digitalcitizen.life/what-google-advertising-knows-about-you/
For Facebook: https://www.wordstream.com/wp-content/uploads/2021/12/wordstream-Facebook-Targeting-Infographic.jpg

BUSINESS MODELS FOR PRIVACY





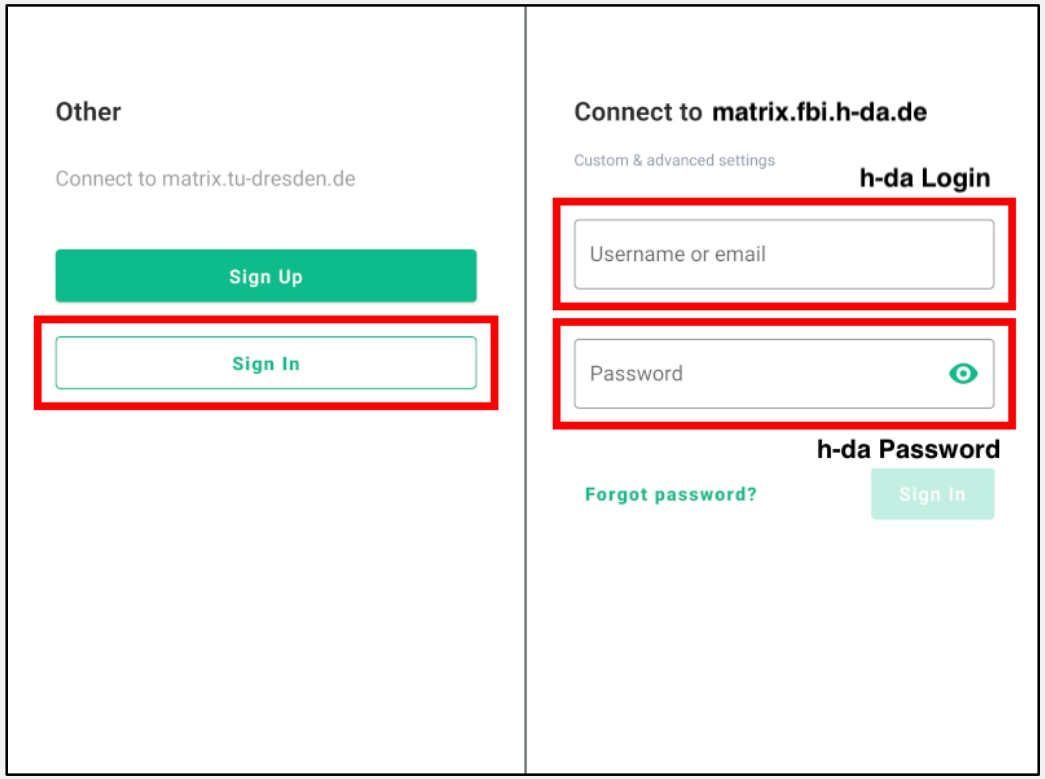
Signal

Contextual ads

Each campaign is matched to the target audience on hand-approved publishers with a combination of **contextual and geographic targeting**.

CHALLENGE: PRIVACY – USABILITY TRADEOFFS

WhatsApp: automated phone book upload & contact discovery



Element / Matrix: manual entry of user name and password

CHALLENGE: INTERDEPENDENT PRIVACY

WhatsApp: automated phone book upload & contact discovery

People's privacy decisions can influence others:

- Bystander privacy
- Uploading others' picture to social media
- Syncing others' personal data into cloud backups
- Entering other's personal data into LLMs / chatbots
- WhatsApp phone upload to sync contacts
- Network effects
- …

Usable privacy research

USABLE PRIVACY RESEARCH

Awareness, Adoption, and Misconceptions of Web Privacy Tools

A Design Space for Effective Privacy Notices

Defending Against the Dark Arts: Recognising Dark Patterns in Social Media

A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web

"My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security

Unwillingness to Pay for Privacy: A Field Experiment

"Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia

Publication venues:

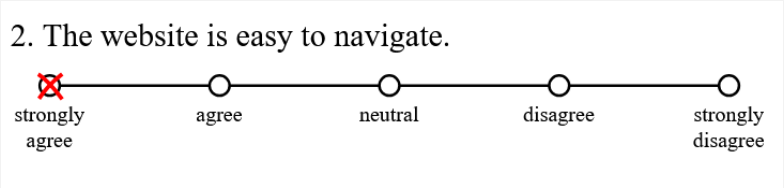
- Proceedings on Privacy-Enhancing Technologies (PoPETs / PETS)
- Symposium on Usable Privacy and Security (SOUPS)
- ACM Conference on Human Factors in Computing Systems (CHI)
- Security & Privacy conferences (USENIX Security, NDSS, ACM CCS, IEEE S&P, ...)
- Workshop on Privacy in the Electronic Society (WPES)
- ...

Fischer-Hübner and Karegar, Overview of Usable Privacy Research: Major Themes and Research Directions, https://doi.org/10.1007/978-3-031-54158-2_3

HCI METHODS

Methods from Human-Computer Interaction (HCI)

- **Quantitative**: numerical data, analysis with mathematical / computational techniques
  Examples: measurements of user interactions, Likert scales and other closed-ended questions in surveys)
- **Qualitative**: non-numerical data that cannot be (meaningfully) quantified, analysis involves identification of recurring patters and themes, categorization, etc.
  Examples: surveys (e.g., open-ended questions), interviews, focus groups, interface analysis, content analysis, …
- **Mixed-method approaches**



Likert scale
(Source: Wikipedia)

EXAMPLE: USER INTERACTIONS WITH CONSENT NOTICES

(Un)informed Consent: Studying GDPR Consent Notices in the Field

Christine Utz
Ruhr-Universität Bochum
Bochum, Germany
christine.utz@rub.de

Martin Degeling
Ruhr-Universität Bochum
Bochum, Germany
martin.degeling@rub.de

Sascha Fahl
Ruhr-Universität Bochum
Bochum, Germany
sascha.fahl@rub.de

Florian Schaub
University of Michigan
Ann Arbor, Michigan
fschaub@umich.edu

Thorsten Holz
Ruhr-Universität Bochum
Bochum, Germany
thorsten.holz@rub.de

ABSTRACT

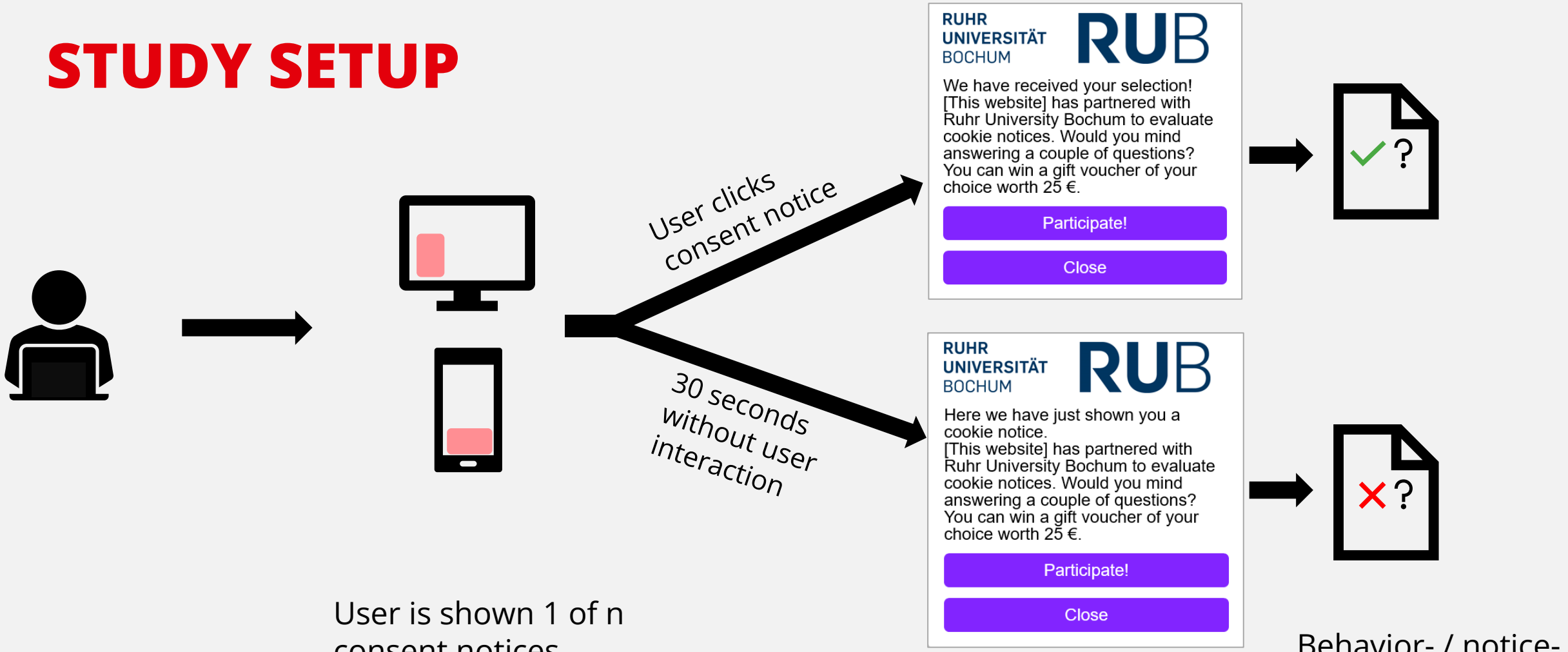
Since the adoption of the General Data Protection Regulation (GDPR) in May 2018 more than 60 % of popular websites in Europe display *cookie consent notices* to their visitors. This has quickly led to users becoming fatigued with privacy notifications and contributed to the rise of both browser extensions that block these banners and demands for a solution that bundles consent across multiple websites or in the browser. In this work, we identify common properties of the graphical user interface of consent notices and conduct three experiments with more than 80,000 unique users on a German website to investigate the influence of notice position, type of choice, and content framing on consent. We find that users are more likely to interact with a notice shown in the lower (left) part of the screen.

ACM Reference Format:
Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3319535.3354212

1 INTRODUCTION

In recent years, we have seen worldwide efforts to create or update privacy laws that address the challenges posed by pervasive computing and the "data economy". Examples include the European Union's General Data Protection Regulation (GDPR) [46], which went into effect on May 25, 2018, and the California Consumer Pri-

STUDY SETUP



User visits website

User is shown 1 of n consent notices.
Plugin measures all interactions with notice

quantitative

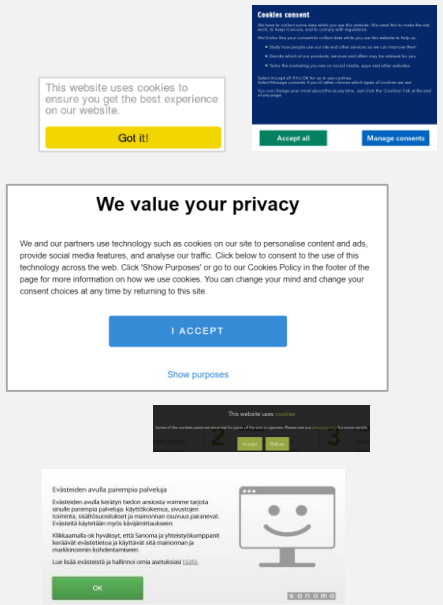
Notice is replaced with invitation to survey

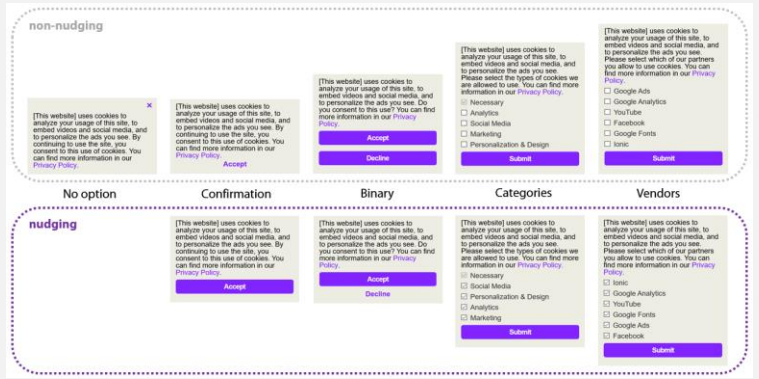
Behavior- / notice-specific survey

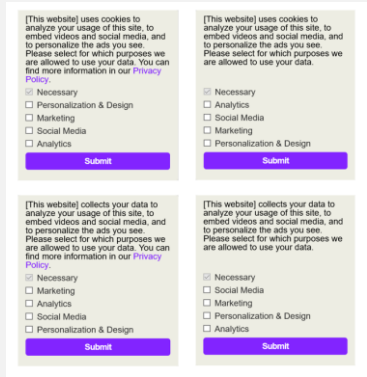
quantitative

qualitative

EXPERIMENTS







Sample & inspect 1000 real-world consent notices, identify design space

Experiment 1: Position

Highest interaction: bottom left

Experiment 2: Choices / nudging

Significant influence of options & nudging

Experiment 3: Privacy policy link / (non-)technical language

Little influence on interaction rates

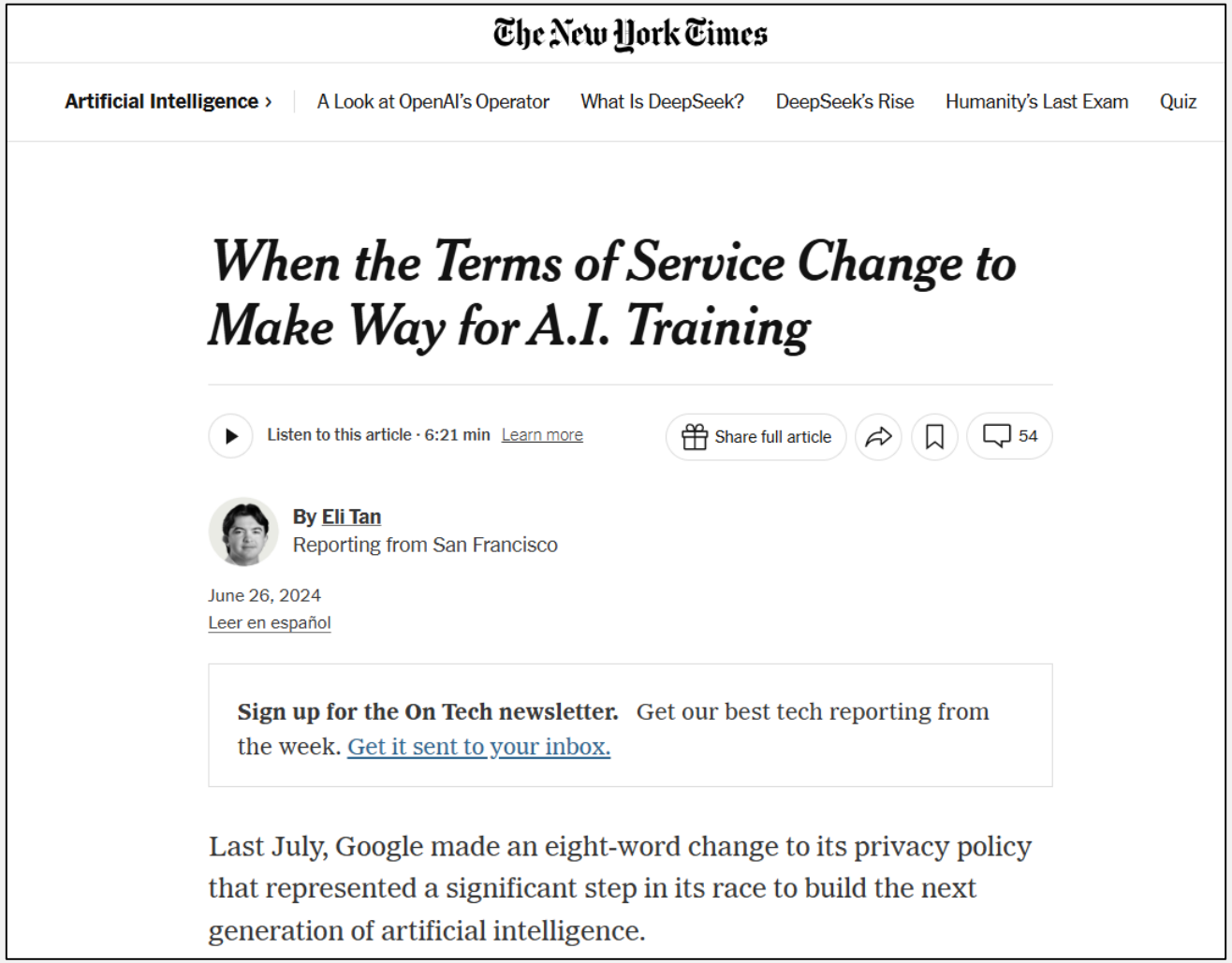
COMMON PITFALLS

- Realism (in-lab vs. field study)
- Ecological validity
- Recruitment, participant sample, selection bias
- Self-reported answers, social desirability bias, **privacy paradox**
- Other biases: agreement bias, order bias, …
- Possible need for **deception** about study purpose
- Research ethics
- …

USABLE PRIVACY IS MULTIDISCIPLINARY

- Computer Science
- UX
- Psychology
- Linguistics
- Law
- Social Sciences
- …

CURRENT TOPICS: AI



The New York Times

Artificial Intelligence › | A Look at OpenAI's Operator | What Is DeepSeek? | DeepSeek's Rise | Humanity's Last Exam | Quiz

When the Terms of Service Change to Make Way for A.I. Training

Listen to this article · 6:21 min Learn more

Share full article 54

By Eli Tan
Reporting from San Francisco

June 26, 2024
Leer en español

Sign up for the On Tech newsletter. Get our best tech reporting from the week. Get it sent to your inbox.

Last July, Google made an eight-word change to its privacy policy that represented a significant step in its race to build the next generation of artificial intelligence.

CURRENT TOPICS: PLATFORM REGULATION

Article 25 Digital Services Act (DSA)
Online interface design and organisation

"Providers of **online platforms** shall not design, organize or operate **their online interfaces in a way that deceives or manipulates** the **recipients of their service** or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions."

Santos et al., Which Online Platforms and Dark Patterns Should Be Regulated Under Article 25 of the DSA?, SSRN Preprint, July 2024, https://dx.doi.org/10.2139/ssrn.4899559

WANT TO LEARN MORE?

christine.utz@ru.nl

https://christineutz.net

I supervise **theses** and **research internships** in …

- Usable privacy & security
- Online tracking & defenses
- Analyzing dark patterns and privacy risks in apps and developer tools
- …