

Defence Against the Dark Patterns

UX Lessons from the Deceptive Side of the Web



PRESENTER

Cat Easdon

Senior Privacy Engineer

Today

- Intro to privacy
- Privacy threat modeling
- Dark patterns
 - Examples
 - Fairer alternatives
 - Legal consequences
- Inclusive privacy
- Privacy challenges in your work



About Me

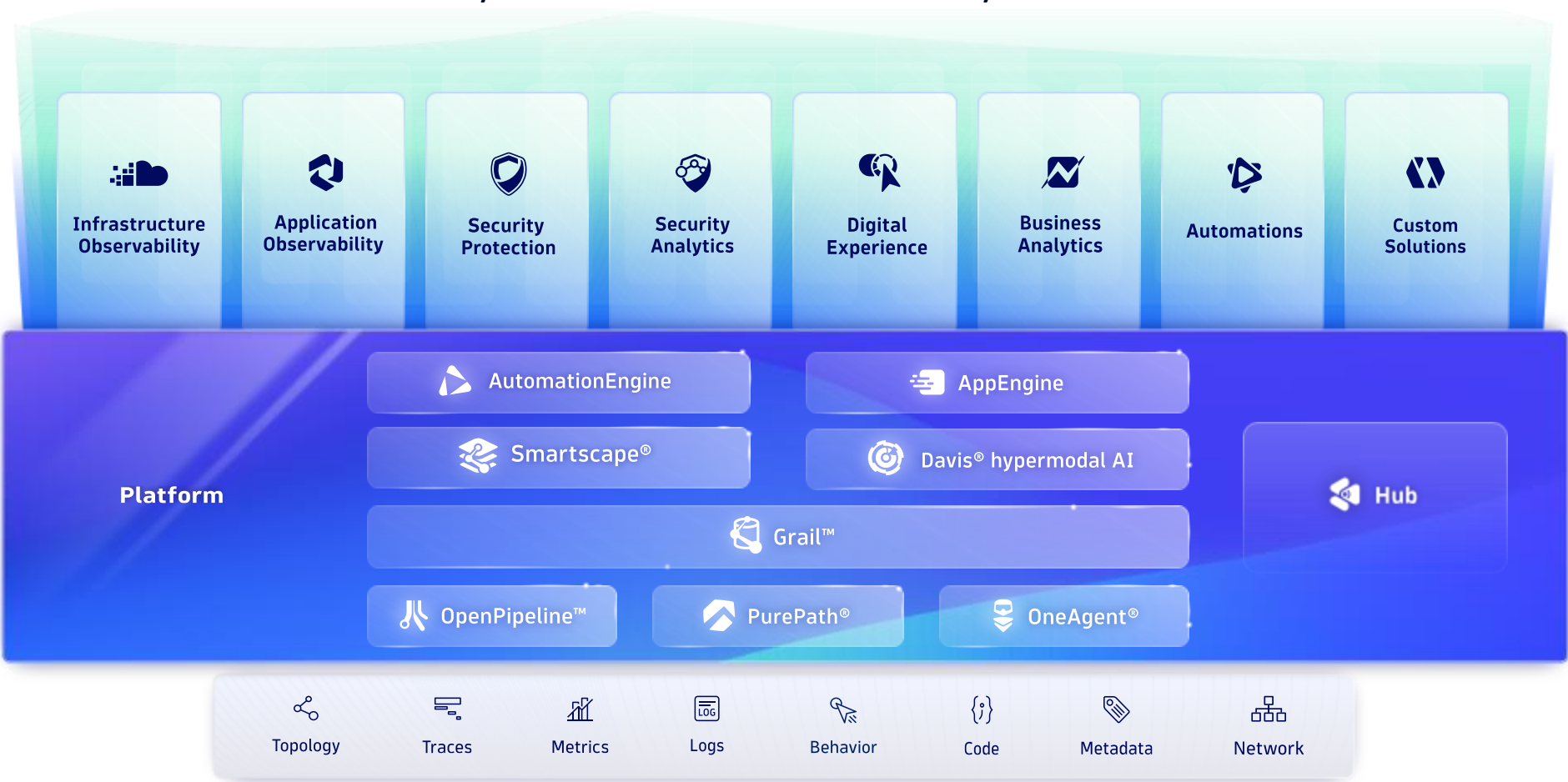
- Senior Privacy Engineer and TechEvangelist at Dynatrace
- 🏔️-obsessed Brit based in Innsbruck
- Outside of work: research and tech policy, trail running, hiking, skiing...
- Previously: hacking CPUs at TU Graz



About Dynatrace



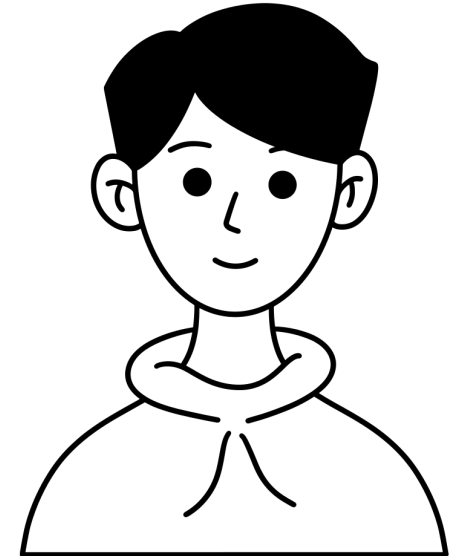
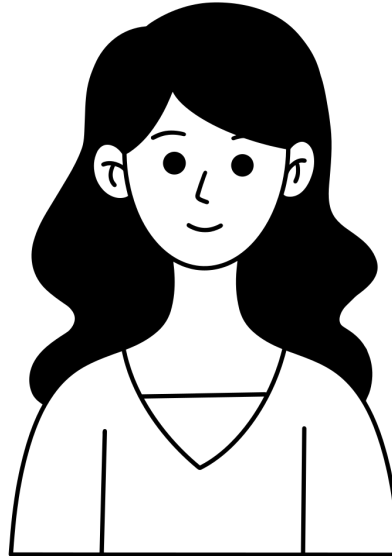
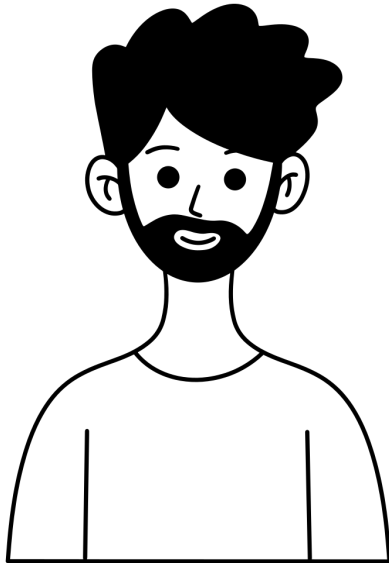
Analytics and Automation for Unified Observability at **CLOUD DONE RIGHT.**



Privacy meets UX

UX Practitioners' Engagement with Privacy

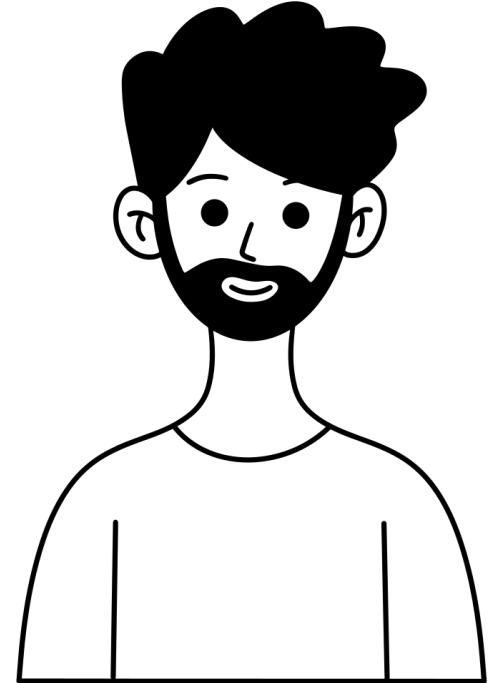
[“Legal Trouble?: UX Practitioners' Engagement with Law and Regulation”](#) (Gray et al., Companion Publication of the 2024 ACM Designing Interactive Systems Conference) interviewed 3 UX practitioners about their experiences



UX Practitioners' Engagement with Privacy

Jacob

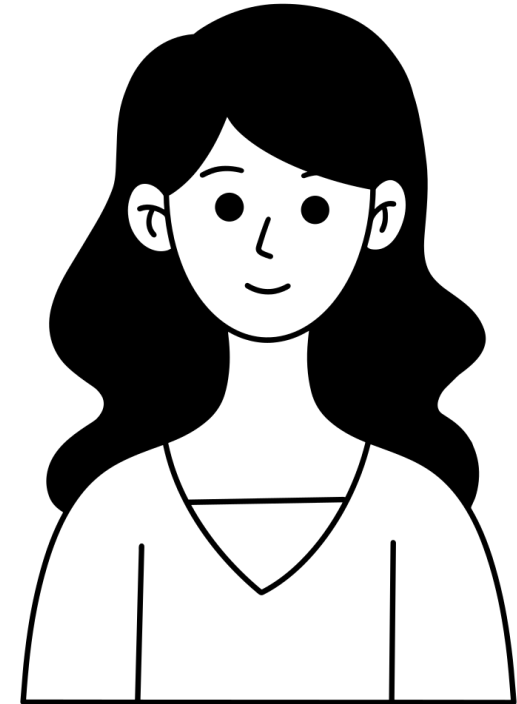
- Tries to persuade developers not to use dark patterns because they're unethical
- Was unaware there are legal implications to using dark patterns
- Company doesn't have a legal team
- There aren't really "any protections" (like internal policies) in place to make sure they're compliant



UX Practitioners' Engagement with Privacy

Amy

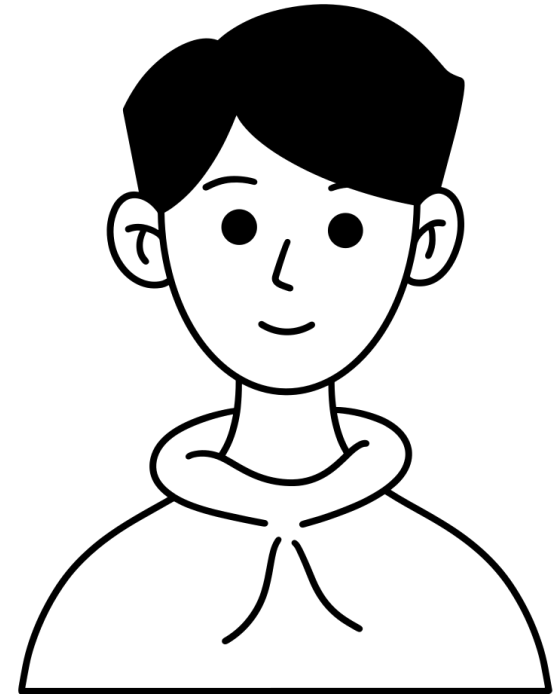
- Privacy is another team's responsibility: her responsibility is advocating for user-centered design
- Work is handed over to a central team for legal checks
- Sees privacy as “legal trouble” that it is important for the company to avoid



UX Practitioners' Engagement with Privacy

Conrad

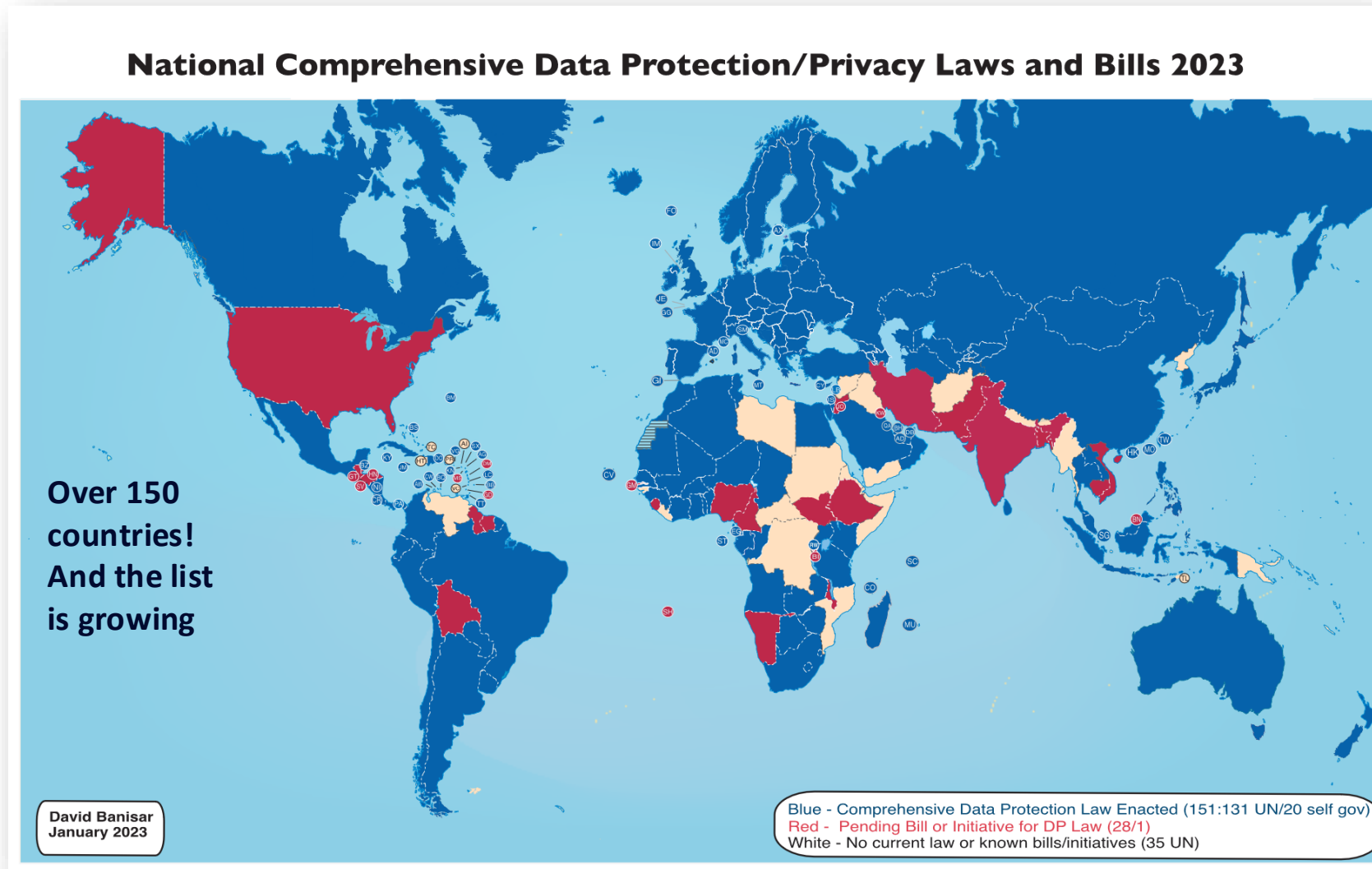
- GDPR is “important” but has added friction to his design workflow
 - To avoid liability, his company now outsources user testing to an external agency
- Would like to have access to a legal expert for advice
- Wary of talking to his company’s legal team as “they are not on our side” and try to block everything



What does privacy mean to you? What contact have you had with it in your UX work?

Intro to Privacy

What Does Privacy Mean?



What Does Privacy Mean?

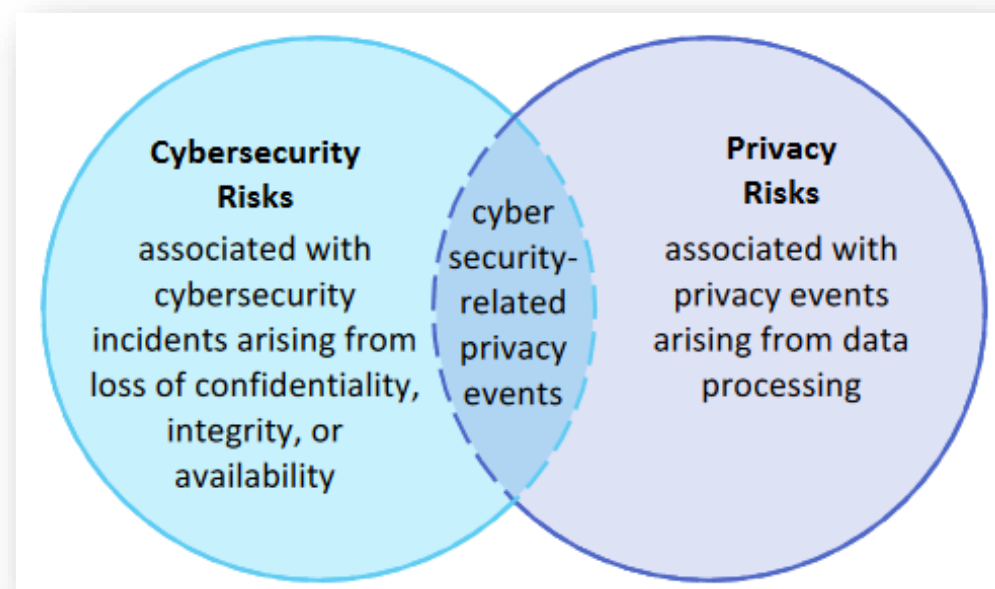
- Right to know, access, export
- Right to update (rectify)
- Right to delete (“be forgotten”)
- Right to data portability
- Plus more...
 - Right to restriction of processing
 - Right not to be subject to automated decision-making, incl. profiling (GDPR)
 - Right to opt out of sensitive data processing (CPRA)



What Does Privacy Mean?

Privacy OWASP Top 10

1. Web Application Vulnerabilities
2. Operator-sided Data Leakage
3. Insufficient Data Breach Response
4. **Consent on Everything**
5. **Non-transparent Policies, Terms and Conditions**
6. **Insufficient Deletion of User Data**
7. **Insufficient Data Quality**
8. Missing or Insufficient Session Expiration
9. **Inability of Users to Access and Modify Data**
10. **Collection of Data Not Required for the User-Consented Purpose**



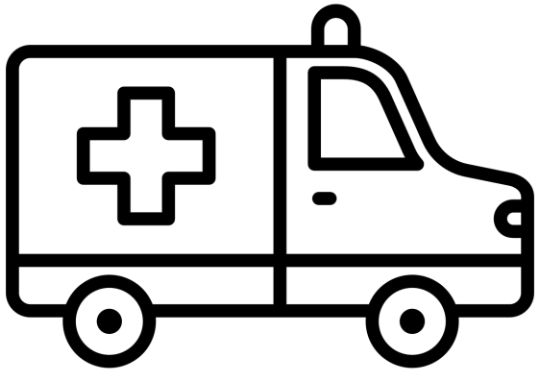
What Does Privacy Mean?



Image: [Gatha Varma](#)

What Does Privacy Mean?

- Privacy isn't about hiding everything!
- Society runs on information flows, but these flows should be *context-appropriate*
- Know your users and their context(s)
 - Which information is it normal to share in this context? In this culture?
 - What do they care about? What are they afraid of?
 - How technically literate are they? Do they understand your product?



Privacy Threat Modeling

What is Threat Modeling?

Anyone can threat model!

It's about answering:

- **What could go wrong?**
- **What are we going to do about it?**
 - Risk = likelihood x impact
 - Cost of mitigation

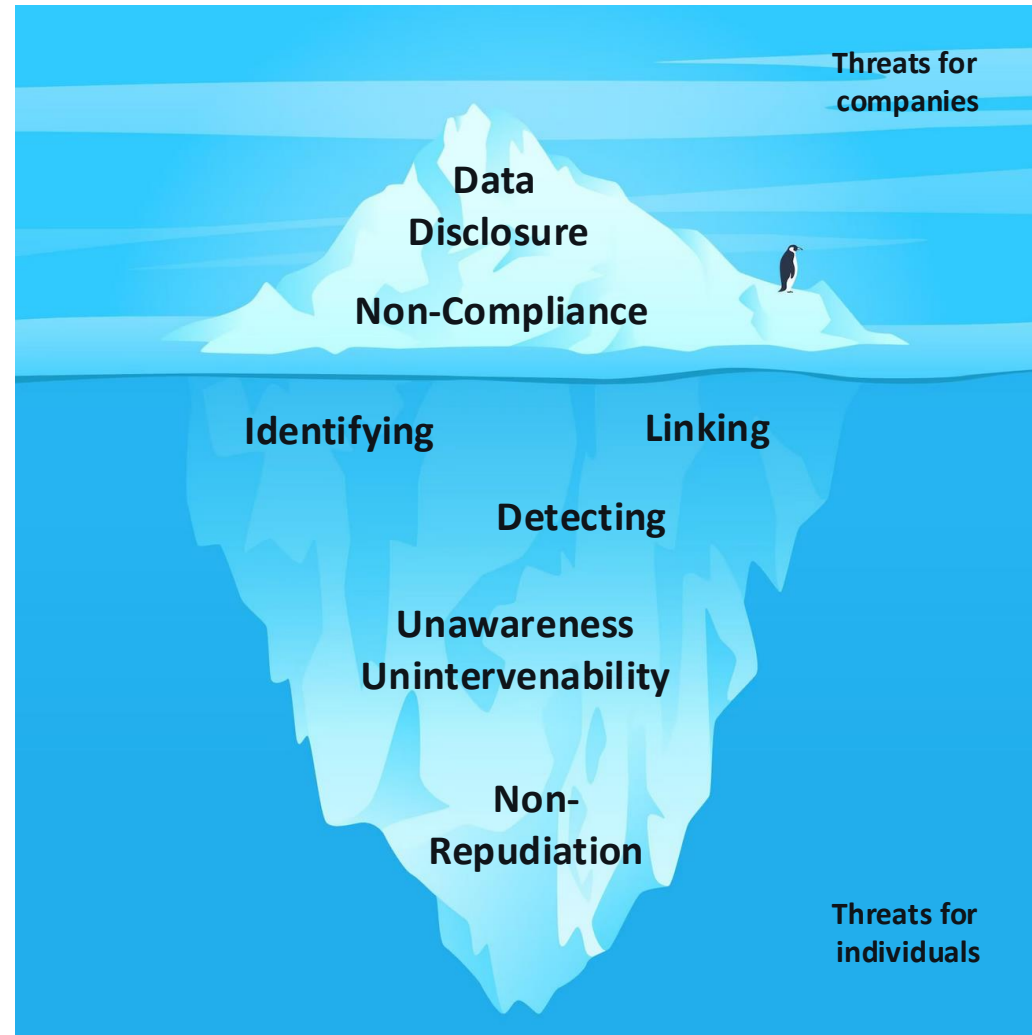
Good starting points:

- [The Threat Modeling Manifesto](#)
- [A Guide to Threat Modeling for Developers](#)



Privacy Threat Modeling: LINDDUN

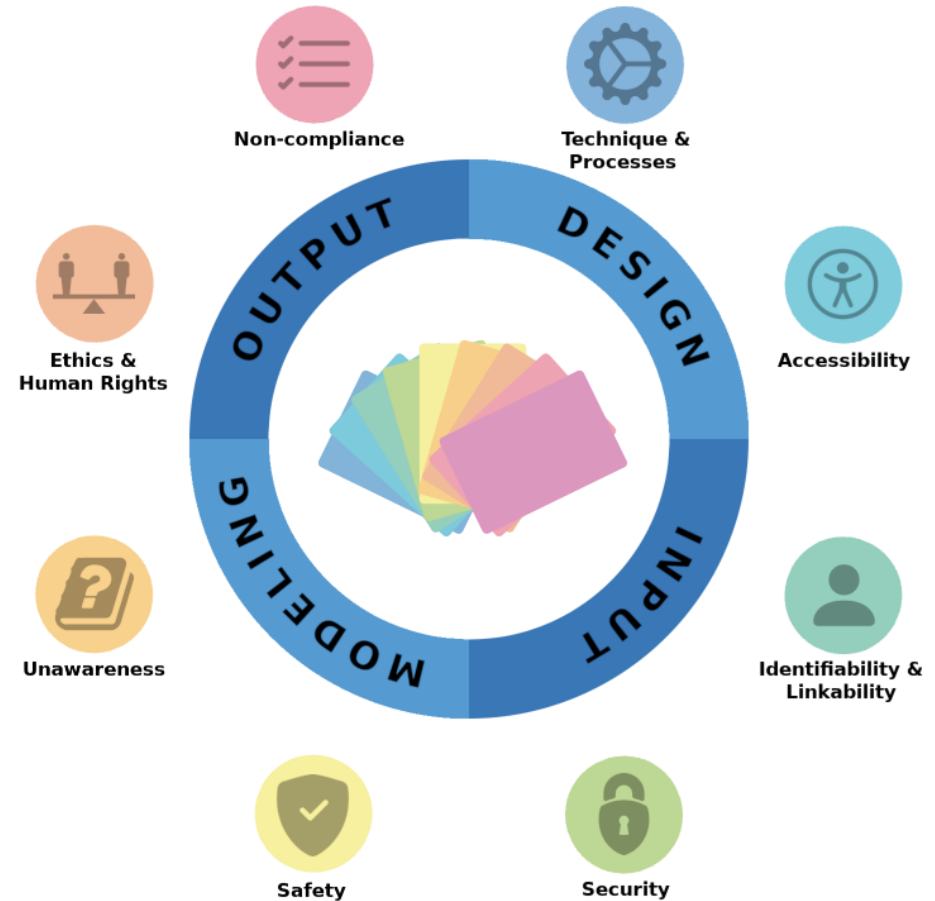
[LINDDUN](#)



- **Linking:** connecting the dots
- **Identifying:** who's who?
- **Non-repudiation:** I know what you did
- **Detecting:** I don't need to read the data to know you're in there
- **Data disclosure**
 - *Not* identical to a breach of confidentiality!
 - Includes collecting unnecessary or excessive data, sharing the data too widely, retaining it for too long...
- **Unawareness & unintervenability:** I had no idea you were doing that and now you won't stop
- **Non-compliance:** that'll be \$5 billion please, Facebook

Privacy Threat Modeling: Plot4AI

- Library of 86 threats relating to AI and ML across 8 categories
- Examples:
 - Are we protected from membership inference attacks?
 - Could the AI system become persuasive, causing harm to the user?
 - Could the AI system limit the right to be heard?
 - Will our AI system make automatic decisions without human intervention?
 - Will any of our users be children?



[Plot4AI](#)

Linkability -> Identifiability -> Non-Repudiation



Hannah Al-Othman
@HannahAlOthman



CPS providing significantly more detail on this case at court — it is understood that the woman had said she did not know how many weeks pregnant she was.

But police gathered **evidence of web searches and messages**, which dispute this.

A 41-year-old woman is facing felony charges in Nebraska for allegedly helping her teenage daughter illegally abort a pregnancy, and the case highlights how law enforcement can make use of online communications in the post-*Roe v. Wade* era.

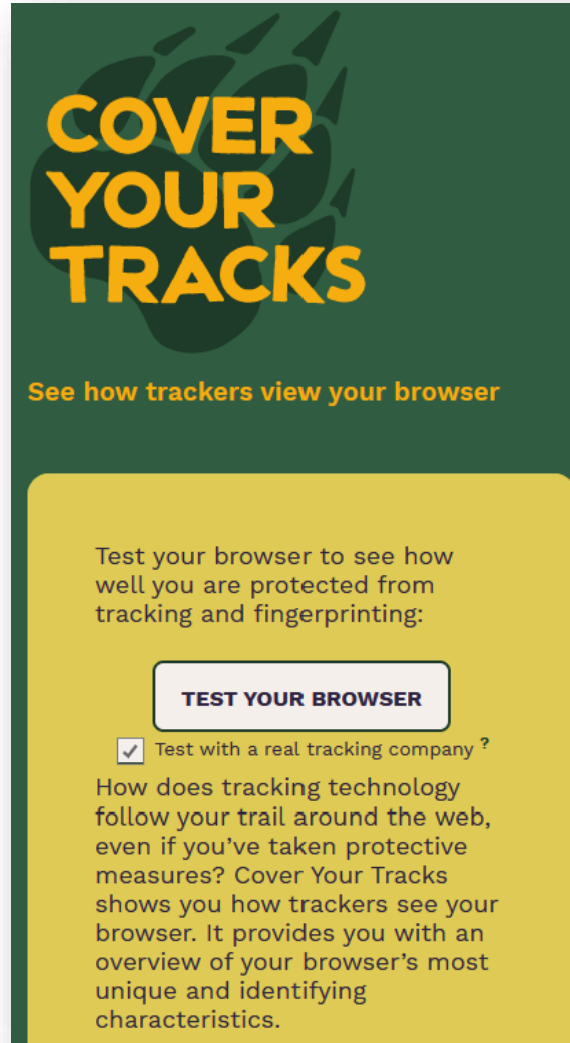
But in mid-June, **police also sent a warrant to Facebook requesting the Burgess' private messages**. Authorities say those conversations showed the pregnancy had been aborted, not miscarried as the two had said.

The messages appear to show Jessica Burgess coaching her daughter, who was 17 at the time, how to take the abortion pills.

"Ya the 1 pill stops the hormones an rhen u gotta wait 24 HR 2 take the other," read one of her messages.



Linkability -> Identifiability -> Non-Repudiation

A promotional banner for 'Cover Your Tracks'. The top half has a dark green background with a faint paw print graphic and the text 'COVER YOUR TRACKS' in large, bold, yellow letters. Below this, in smaller yellow text, is 'See how trackers view your browser'. The bottom half has a yellow background with black text. It starts with 'Test your browser to see how well you are protected from tracking and fingerprinting:', followed by a button labeled 'TEST YOUR BROWSER'. Below the button is a checked checkbox and the text 'Test with a real tracking company?'. The final paragraph explains that the tool shows how trackers see the browser and provides an overview of its unique characteristics.

COVER YOUR TRACKS

See how trackers view your browser

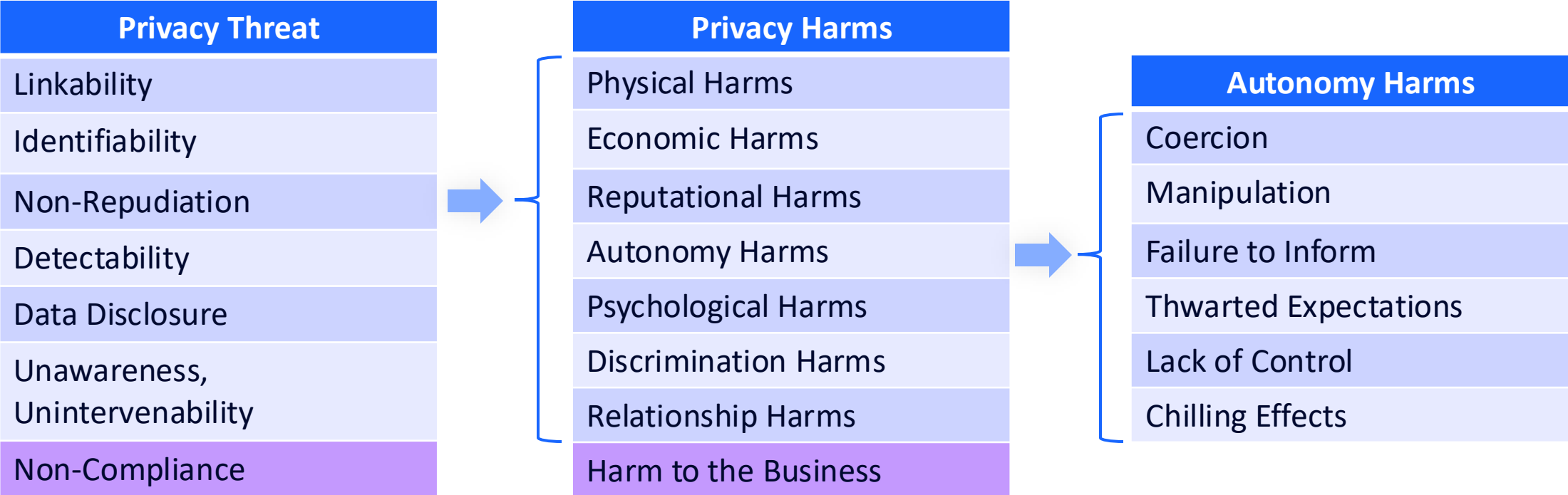
Test your browser to see how well you are protected from tracking and fingerprinting:

TEST YOUR BROWSER

☒ Test with a real tracking company ?

How does tracking technology follow your trail around the web, even if you've taken protective measures? Cover Your Tracks shows you how trackers see your browser. It provides you with an overview of your browser's most unique and identifying characteristics.

Privacy Harms



[Privacy Harms](#), Citron & Solove, Boston University Law Review (2022)



Privacy Harms: Manipulation

Neuroticism - Trapped Neuroticism - Stress Reactors Neuroticism - Self Lovers
Neuroticism - Easily Deflated Neuroticism - Internal Escapists
General Attitudes - I generally get a raw deal out of life Dealing with Stress - Hot and Cold
Dealing with Stress - Emotional Dealing with Stress - Bottled Up

Clickagy > Health > **Addictions** > Alcohol

Skydeo > ConditionGraph > Disease Propensity by Type > **Depression** Diagnosis

adready_drug_rehab (Grapeshot)

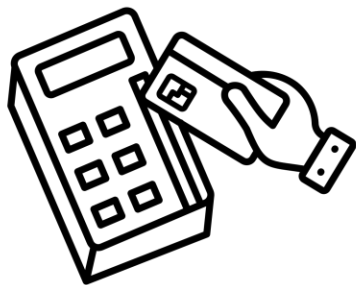
VisualDNA Lifestyle - Lifestyle - Health - Trying to cut down on **Alcohol**

Data provider: Nielsen Marketing Cloud

TransUnion - Demographics - Marital Status - Likely Recently **Divorced**

AlikeAudience: United States > Interest > Entertainment > Party And **Night Club** Enthusiasts

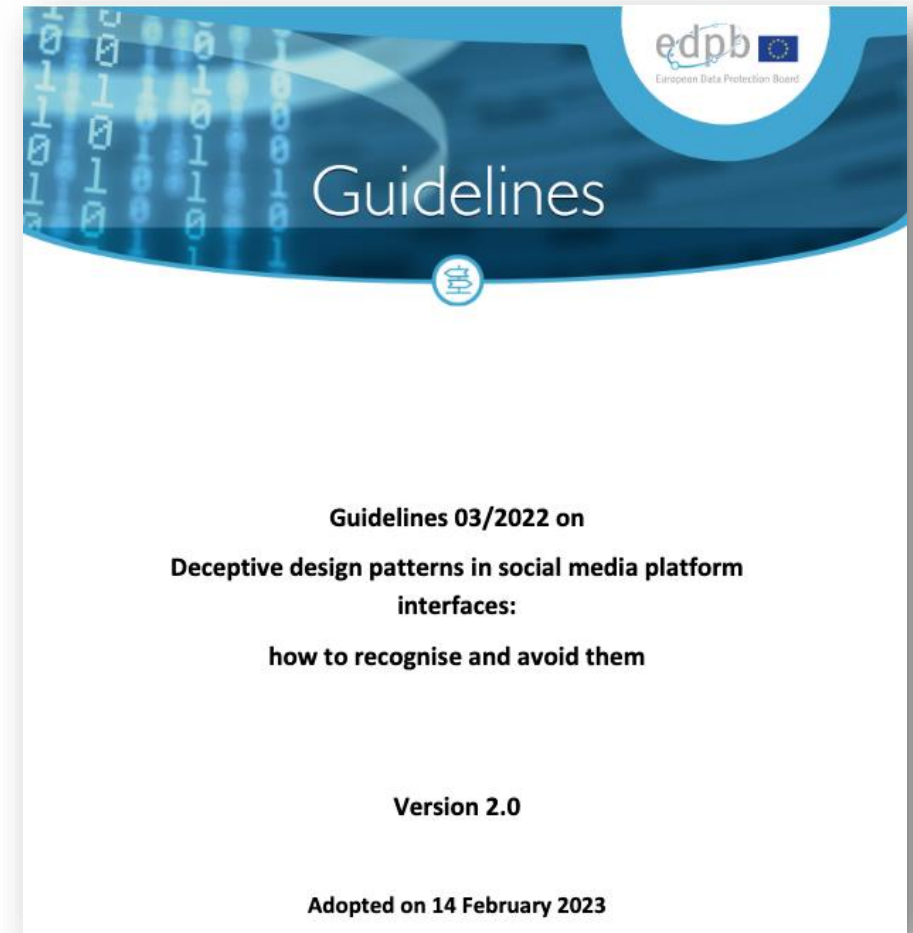
Eyeota - US Acxiom - CPG - **Alcoholic** Drinks - Vodka Brand - Grey Goose for age 21+ - Likely



Dark Patterns

Dark Patterns and Privacy

- Concept introduced in 2010 by UX professional Harry Brignull
- Just design patterns – but sinister ones! Deceive or manipulate users
- Violate the GDPR principles of fairness and transparency + Article 25 (data protection by design and default)
- Also relevant beyond the EU, see e.g.
 - [US FTC's report on dark patterns](#)
 - [Deceptive Patterns Hall of Shame](#), [Fair Patterns](#), and [Privacy Patterns](#)
 - India's ban list (more on this later!)



Pattern 1: Stirring (influencing)

Influencing users' privacy choices by appealing to emotion or using visual nudges.

- Emotional steering
- Hidden in plain sight

Save 15% off your first order!

Enter your email address here.

Confirm

No, I hate saving money.

Sign-up

Just one more step to join your friends!

Your birthdate

Day Month Year

29 12 1996

Share it with no one

Share it with my friends

Share it with everyone

Join the network!

Skip this step and sign up

Pattern 2: Overloading

Exhausting the user so that they give up trying to control how their personal data is used.

- Continuous prompting
- Privacy maze
 - Labyrinth – “the Iliad flow”
- Too many options


The screenshot shows a 'Follow settings' dialog box with a close button (X) in the top right corner. It is divided into several sections:

- News Feed**: Choose how you'll see posts from this Page in your News Feed.
 - Default**: You'll see all posts in their usual order. (Selected with a blue radio button)
 - Favourites**: You'll see posts higher in your Feed. (Radio button)
 - Unfollow**: You won't see this Page's posts in your feed. (Radio button)
- Notifications**: Choose what types of posts you want to be notified about.
 - Content**: Highlights (Right arrow)
 - Video**: Highlights (Right arrow)
 - Live video**: Highlights (Right arrow)
 - Offers**: All limited-time discounts and promos (Toggle switch)
- Unlike this Page**: You won't see their posts in your feed and you'll no longer like this Page. (Toggle switch)


At the bottom, there are two buttons: 'Cancel' (light blue) and 'Update' (blue).

E-Commerce Case Study: Stirring + Overloading


Choose your seat preference


**Option 1: Sit where you want**


or


**Option 2: Select seats later**


Our seat sections

**Extra legroom up front**
ROW 1

**Get off quick**
ROWS 2-5

**Best value up front**
ROWS 6-11

**Stretch out for less**
ROWS 12-13

**Best value at the back**
ROWS 14-30

[Our seats policy explained](#)

A

B

C

D

E

F

1

2

3

4

5

6

7

EXTRA LEGROOM UP FRONT - €21

GET OFF QUICK - €14

BEST VALUE UP FRONT - €10

Recommended

Select your own

Our best value seats

Check-in 60 days pre-departure

Zagreb to Brussels Charleroi

Passengers

AA


aa aa

No window

11A


€8.00

Add recommended seats

 30


E-Commerce Case Study: Stirring + Overloading

Choose your seat preference



Option 1: Sit where you want


or



Option 2: Select seats later


Before continuing without a seat please be advised

If you don't choose seats you will only be able to check-in 24 hours prior to departure where we will randomly allocate you a seat.




Avoid middle seat

Most of our passengers choose their seat so we have less window and aisle seats to allocate at check in.



Seat availability

The longer you wait the less likely you'll get the seat that you want.




Best price now

Our cheapest seats are most likely to sell out quickly. Select seats now to avail of the best price.


Select seats now

Continue without a seat






31

E-Commerce Case Study: Stirring + Overloading



You have chosen random seat allocation

This means:

-  You can only check in 24hrs before each flight
-  You may be seated anywhere in the aircraft
-  You may be allocated a middle seat

[Select seats now](#)

[Continue with random allocation](#)

Pattern 3: Skipping

Trying to make the user forget or overlook the privacy implications of an action.

- Privacy-invasive settings enabled by default
- Distraction tactics: “Look! A free trial!”

Instead:

- Try to build trust with the user and be transparent with them -->



Pattern 4: Obstructing

Making it difficult or impossible to get information about or manage your personal data.

- Dead end
 - Broken or missing link
 - Privacy options are scattered across different menus
- Longer than necessary
 - Extra wait if you click 'Reject all cookies'
- Misleading action

⚠ We cannot update your preferences because they are available only to residents covered by applicable state law. Please review/update your profile address information, revisit this page, and retry your submission.

Your Privacy Rights

Hello inelligible,

If you live outside of the U.S., please visit the [Individual Rights Portal](#) for information about how to exercise your Individual Rights.

Pattern 5: Fickle

Using an inconsistent UI to make it hard for users to understand what's happening with their data.

- Lacking hierarchy
- Decontextualizing
- Inconsistent interface
- Language discontinuity

Examples:

- Privacy policy is a confusing mess and only available in English
- Privacy settings are in different places on desktop vs. mobile, or keep being moved around

Below are translations of this document into other languages. In the event of any conflict, uncertainty, or apparent inconsistency between any of those versions and the English version, this English version is the controlling version.

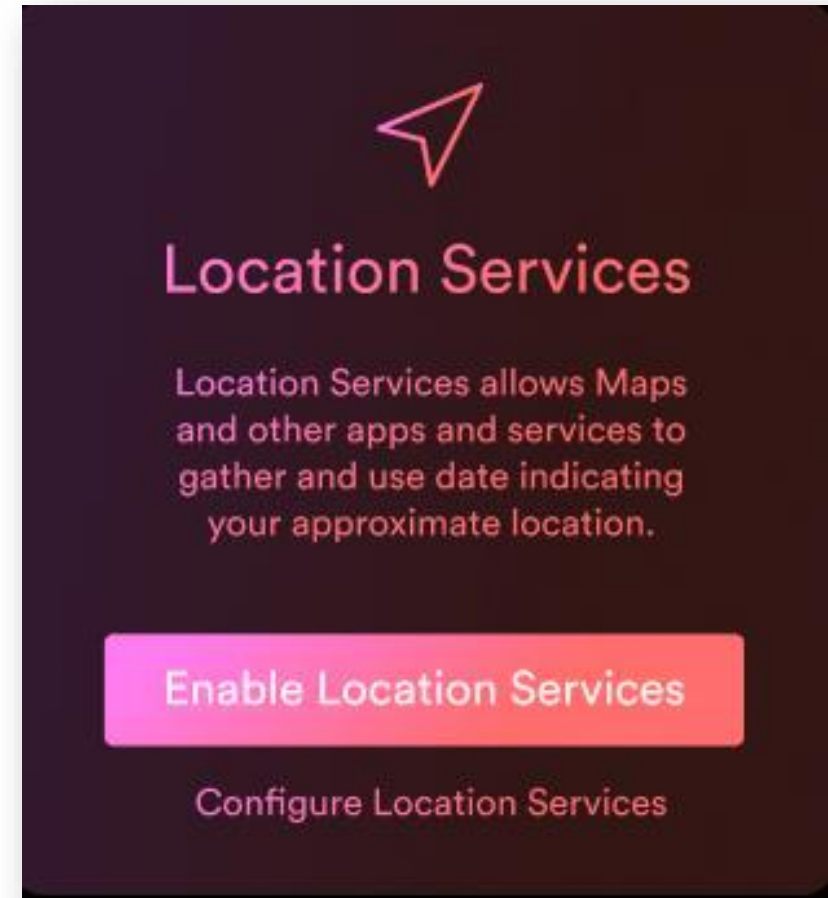
Pattern 6: Left in the Dark

Hiding privacy information and controls or presenting them in a misleading way.

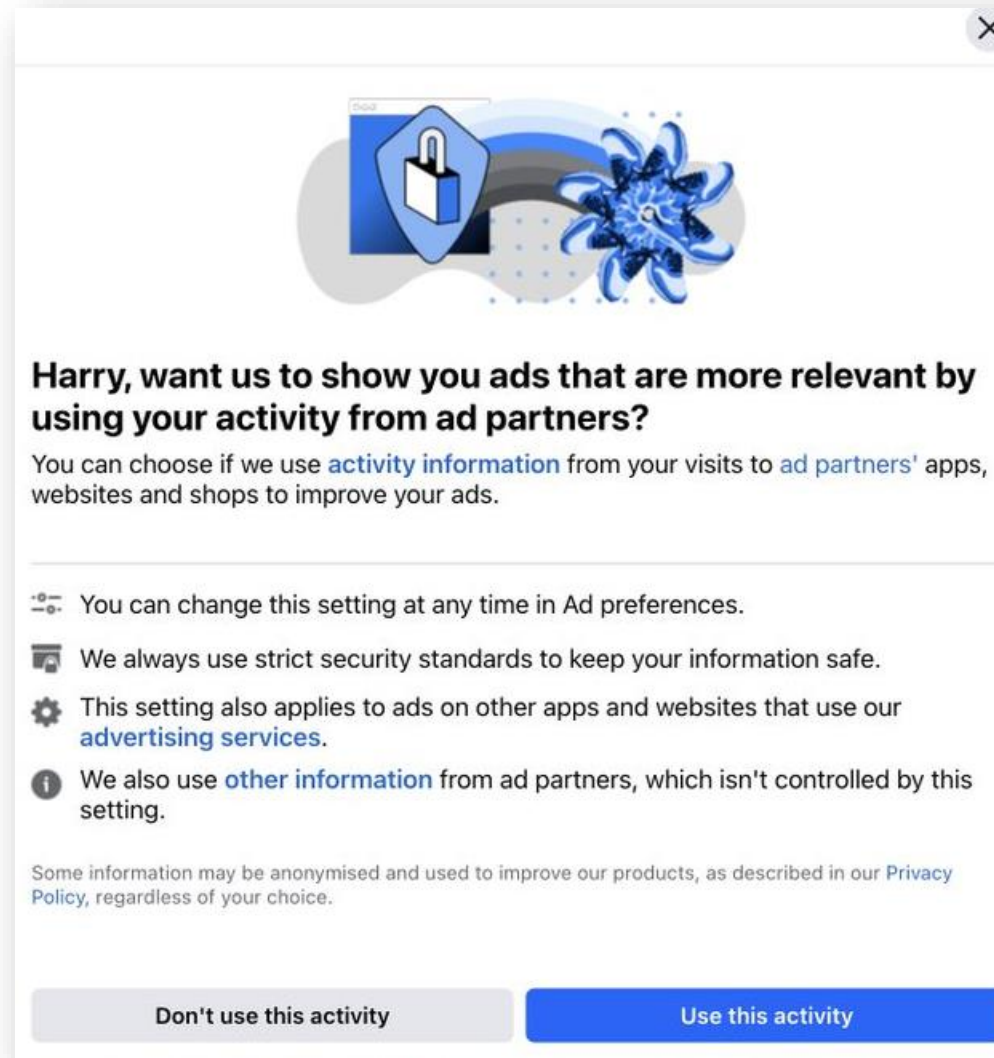
- Conflicting information
- Ambiguous wording or information

Avoid by:

- Improving learnability of the UI
- Just-in-time presentation of documentation
- Minimize the number of concepts you assume your users understand



Case Study: Left in the Dark



Where have you seen dark patterns in action?

India's Ban List

India's Banned Dark Patterns

False Urgency

Stirring

Confirm Shaming

Stirring

Interface Interference

Stirring

Forced Action

Obstructing

Bait and Switch

Fickle

Disguised Ads

Fickle

India's Banned Dark Patterns

Nagging

Overloading

Trick Question

Left in the dark

Subscription Traps

Billing-specific

Drip Pricing

Billing-specific

Basket Sneaking

Billing-specific

Rogue Malware

Hopefully not relevant for our work!

Case Study: Trick Question

EMAIL TYPE	OPT OUT
Recommendations Trendy or popular features, templates, and other creative contents.	<input type="checkbox"/> NO <input checked="" type="checkbox"/> YES
Product Updates News about new features, product updates or changes, etc.	<input type="checkbox"/> NO <input checked="" type="checkbox"/> YES
Marketing News about promotions, events, and other campaigns.	<input type="checkbox"/> NO <input checked="" type="checkbox"/> YES

Save Preferences



E-Commerce Case Study: Adobe's Subscription Trap

Your free trial includes full versions of Adobe apps.

Individuals

Business

Students & Teachers



Creative Cloud All Apps Plan

Get 20+ Creative Cloud apps including Photoshop, Illustrator, InDesign, Premiere Pro and Acrobat Pro.

Plus:

- Step-by-step tutorials
- 100 GB of cloud storage
- Adobe Portfolio and Adobe Fonts

[See apps included](#)

7 days free, then
£49.94 /mo

[Start free trial](#)



E-Commerce Case Study: Adobe's Subscription Trap

Subscription and cancellation terms

Your eligibility to use an Adobe free trial offer is determined solely by Adobe. Your access to any free trial offer is provided at Adobe's sole discretion.

Subscription Terms:

Your subscription begins as soon as your initial payment is processed. Your subscription will automatically renew annually without notice until you cancel. You authorize us to store your payment method(s) and to automatically charge your payment method(s) every month until you cancel. We will automatically charge you the then-current rate for your plan, plus applicable taxes (such as VAT or GST if the rate does not include it), every month of your annual contract until you cancel.

Cancellation Terms:

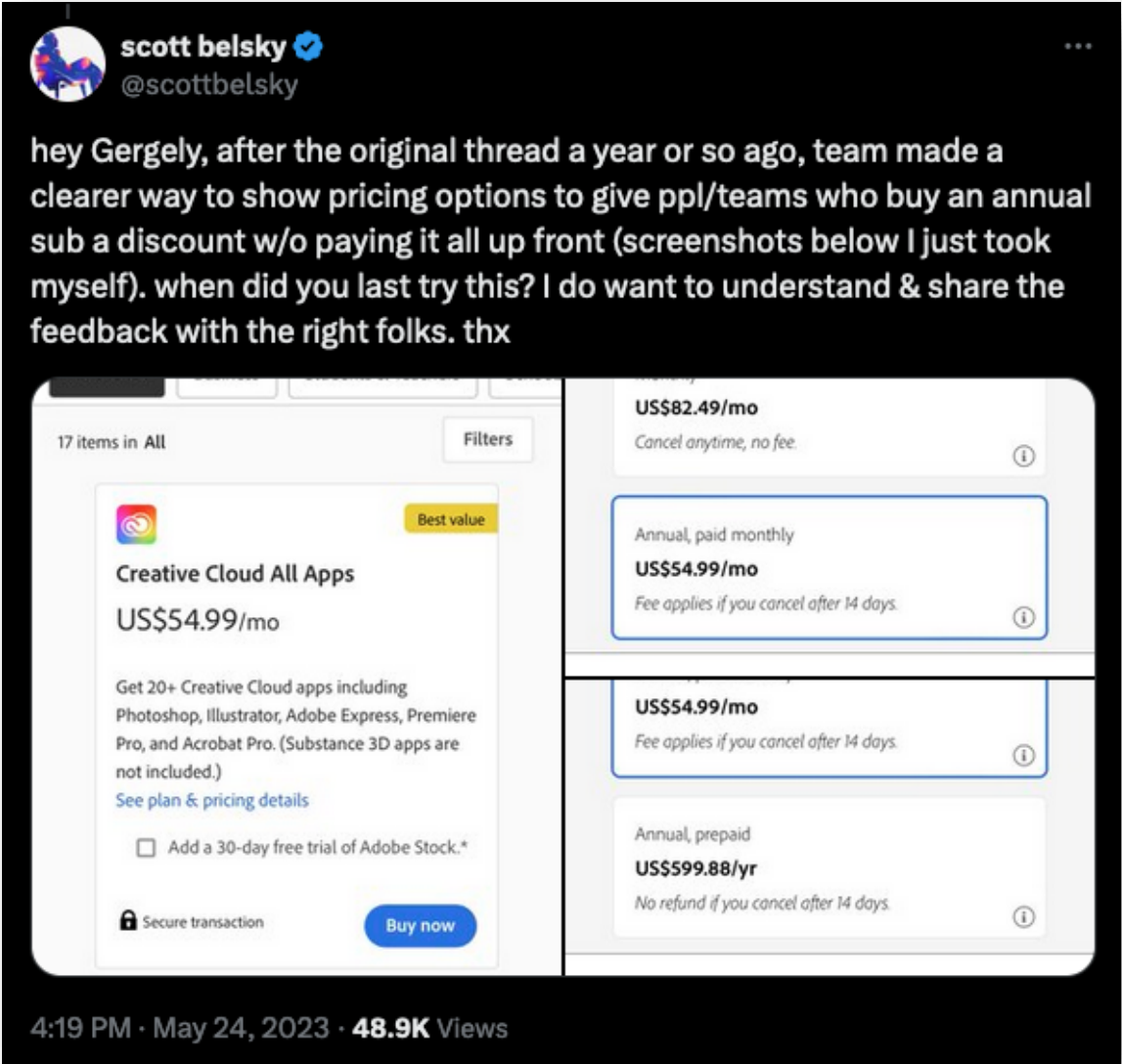
You can cancel your subscription anytime via your [Adobe Account](#) page or by contacting [Customer Support](#)*. If you cancel within 14 days of your initial order, you'll be fully refunded. Should you cancel after 14 days, you'll be charged a lump sum amount of 50% of your remaining contract obligation and your service will continue until the end of that month's billing period.

* Specific countries require cancellations to be made only by contacting [Customer Support](#). See the list of countries [here](#).

Close



E-Commerce Case Study: Adobe's Subscription Trap





Cookies from the Dark Side

Cookies from the Dark Side



You're in control of your cookies

We and our [partners](#) use cookies and process personal data such as your IP address on this site. Some cookies are necessary to run the site and some are optional. Cookies are used to:

Store and/or access information on a device



Personalised ads and content, ad and content measurement, audience insights and product development



Actively scan device characteristics for identification



If you're okay with these purposes, click 'Fine By Me!' below; this will allow us to personalise your website experience. For more information or to change your cookie settings, click 'Cookie Settings'. You can withdraw your consent at any time by visiting Cookie Settings in the footer. To learn more, read our [Privacy and Cookie Policy](#).

[Cookie Settings](#)

[Fine By Me!](#)



Cookies from the Dark Side



Više o našim Politikama zaštite privatnosti te Politikama kolačića možete pročitati ovdje: [Politika zaštite privatnosti](#) , [Politika kolačića](#). Korištenje kolačića može dovesti do prijenosa podataka u zemlje izvan područja EU. Za prijenos podataka u određenim slučajevima potreban nam je vaš pristanak.

Uz vaš pristanak, mi i [naš 846 partneri](#) koristimo kolačiće ili slične tehnologije za pohranu, pristup i obradu osobnih podataka kao što su Vaša posjeta ovoj web stranici, IP adrese i identifikatori kolačića. Neki partneri ne traže Vaš pristanak za obradu Vaših podataka i oslanjaju se na svoj legitimni poslovni interes. Možete povući svoj pristanak ili se usprotiviti obradi podataka na temelju legitimnog interesa u bilo kojem trenutku klikom na "Saznajte više" ili u našoj Pravilima o privatnosti na ovoj web stranici.

Mi i naši partneri obrađujemo podatke kako slijedi:

Personalizirano oglašavanje i sadržaj, mjerenje oglašavanja i sadržaja, uvidi u publiku i razvoj usluga, Pohrana i/ili pristup podacima na uređaju, Precizni geolokacijski podaci i identifikacija putem skeniranja uređaja, Prijenos podataka

Saznaj više

Prihvati i zatvori

Cookies from the Dark Side

Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising. Accept all cookies to indicate that you agree to our use of cookies on your device. [Atlassian cookies and Tracking notice](#)

Preferences

Only necessary

Accept all

Cookies from the Dark Side

Disclaimer

The rules of the Bar Council of India prohibit law firms from advertising and soliciting work through communication in the public domain. This website is meant solely for the purpose of information and not for the purpose of advertising. Lakshmikumaran & Sridharan does not intend to solicit clients through this website. We do not take responsibility for decisions taken by the reader based solely on the information provided in the website. By clicking on 'ENTER', the visitor acknowledges that the information provided in the website (a) does not amount to advertising or solicitation and (b) is meant only for his/her understanding about our activities and who we are.

I AGREE

EXIT SITE

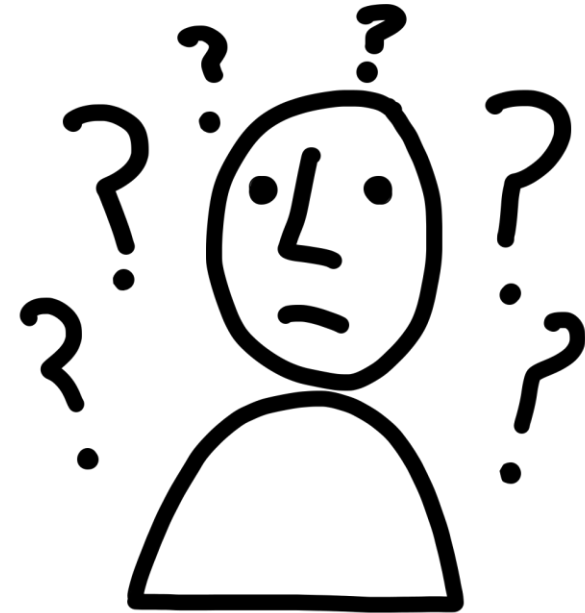
By continuing to use this site you consent to the use of cookies on your device as described in our [Cookie Policy](#)

What are the worst cookie dialogs you've seen? How do they compare to other cases of dark patterns?

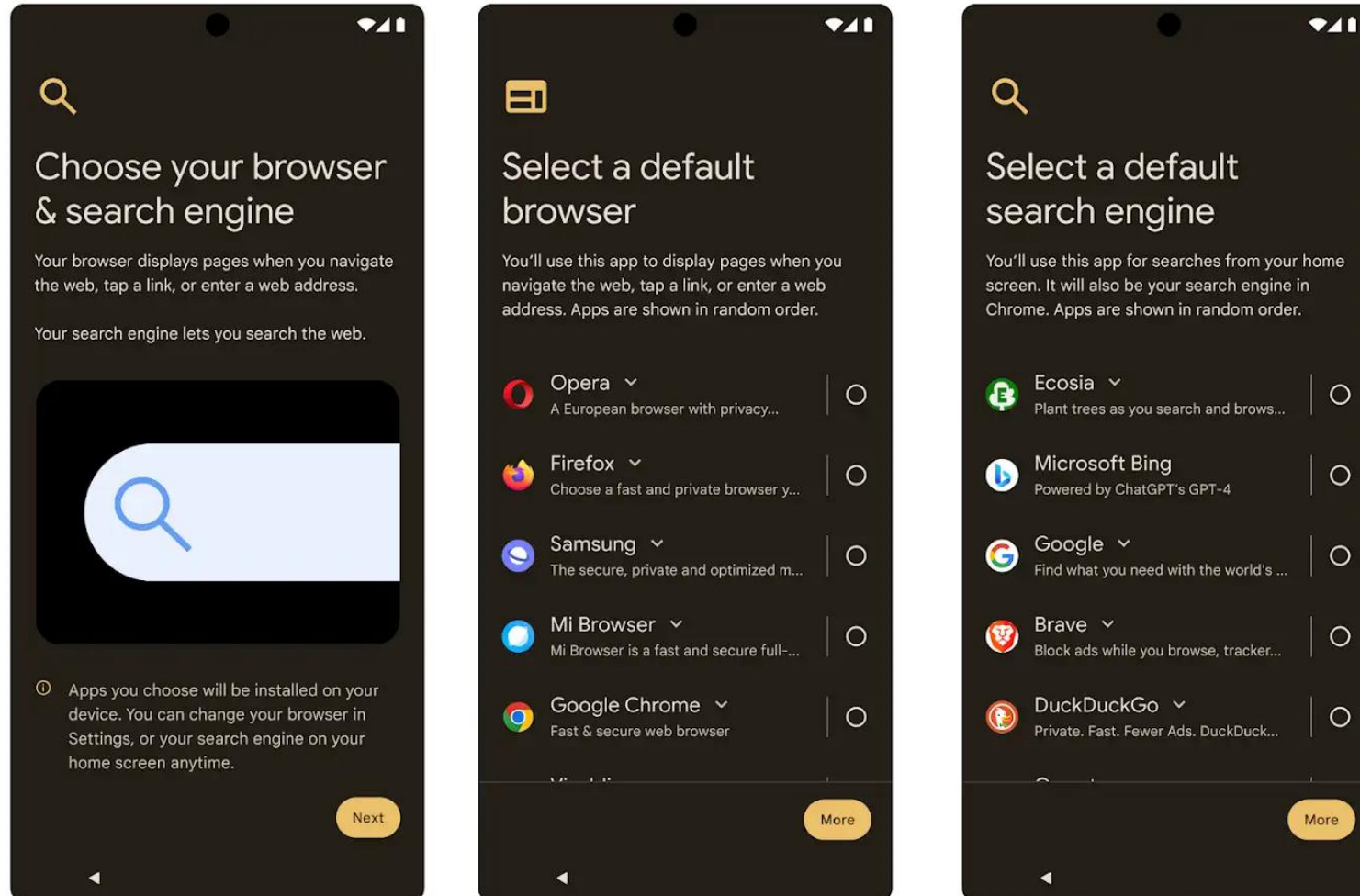
Inclusive Privacy

Users Have Different Privacy Needs

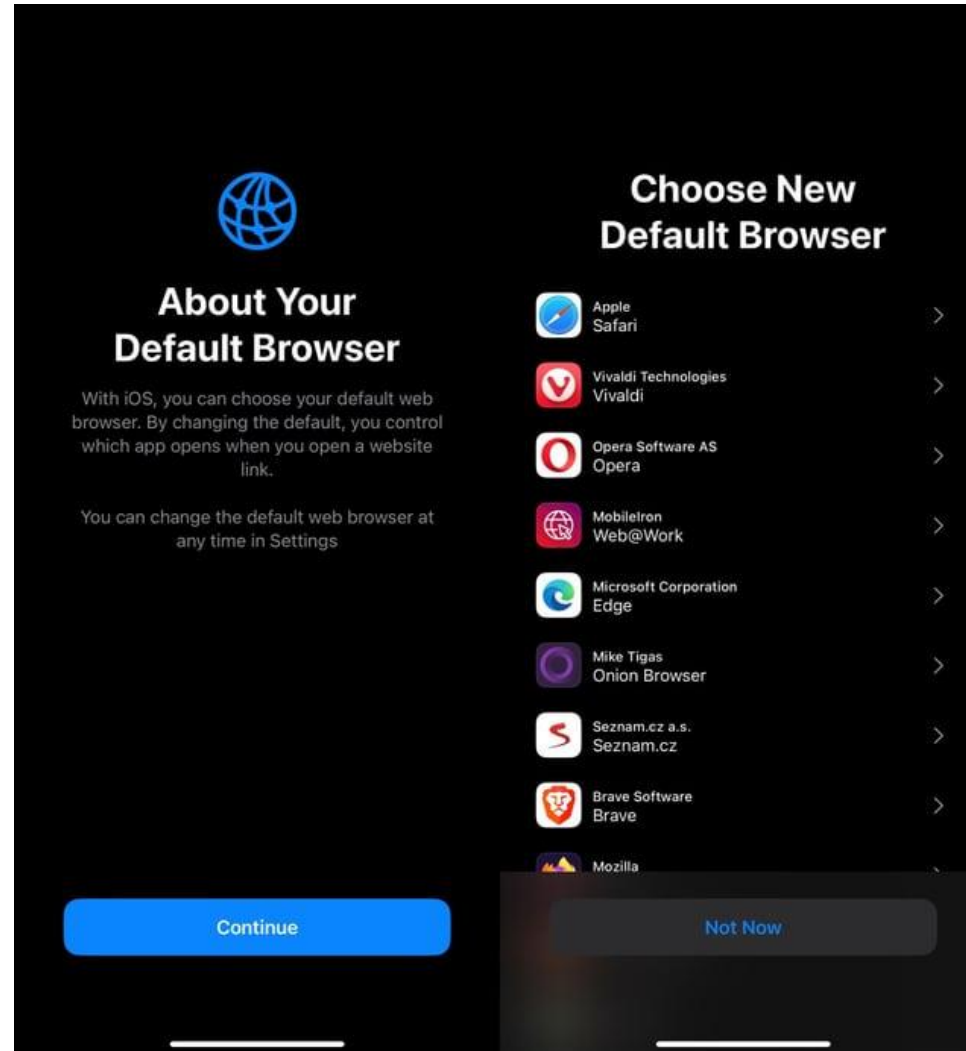
- Not only are their threat models different...
- But also their awareness and understanding of privacy
- And their understanding of tech in general!
 - *“What’s a browser?”*
 - *“What’s end-to-end encryption?”*
- Many users don’t understand what they’re consenting to or the choices they’re being asked to make



“Free Choice” of Browser and Search Engine: Android



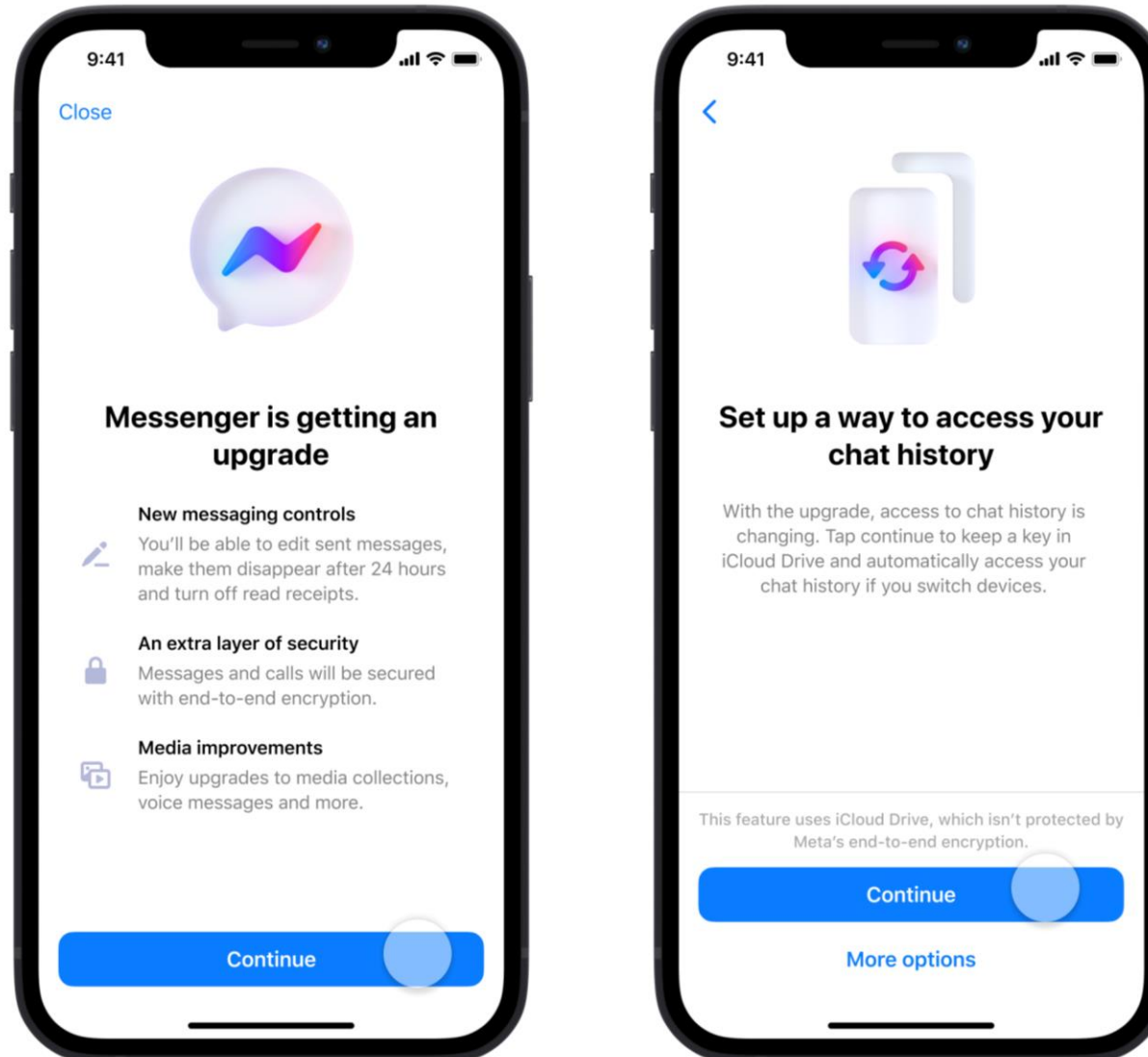
“Free Choice” of Browser: iOS



“Free Choice” of Browser: The Reality

We asked people what they think happens after they choose a default browser. **Only about half (52%) of people understand that their default browser is opened when they, for example, click on a link in an email or document.**⁶⁰ This share did not significantly vary across treatment groups, which is surprising as the Q&A screen (displayed to T2-4) explicitly states this is what happens when they select a default browser. Moreover, 6% of people incorrectly believe that they are *only* able to use their default browser (i.e., that all other browsers would be disabled). Even more significantly, **over half (53%) also erroneously believed that their default browser would automatically be pinned to their taskbar.** Previous research suggests this is a common misconception - and the impact of not being pinned to the taskbar, in terms of how this impacts people's usage of browsers, is an area where we consider further research could be undertaken.

“Free Choice” on Facebook Messenger



“Free Choice”: The Bundeskartellamt’s Opinion

II. Free and Informed Choice Options

4. Google undertakes to design the choice options to be offered to Users pursuant to para. 1 under these Commitments in a way that Users can provide consent in a freely given, specific, informed, and unambiguous manner.

5. Google commits in this regard in particular to design the choice options to be offered to Users pursuant to para. 1 for cross-service data processing in a transparent manner. This requires that Users are informed about the consent options in an intelligible and easily accessible form, using clear and plain language. This entails in particular:

- providing Users with concrete information on the choices to be offered to them with regard to cross-service data processing, including specific information on the circumstance, the purpose and the manner of the cross-service data processing, and - if this is the case - to what extent cross-service data processing also takes place without offering a consent option,
- setting up the choice options in a technical and/or visual manner to ensure that it is not too complex for Users to easily understand them, in particular when using multi-step consent processes,
- designing the choice options in a way that it is clear to the Users how the consent options relate to each other,
- phrasing the choice options objectively.

“Free Choice”: The Bundeskartellamt’s Opinion

6. Where Google asks Users for consent in line with para.1, Google will not make it easier for Users to give consent to cross-service data processing than not to give it. This includes in particular:

- a. Ensuring that visually, the option to reject cross-service data processing is presented at least equally to the option to consent, in particular in terms of colour, layout or font size;
- b. Ensuring that technically, the option to reject cross-service data processing is designed at least equally to the option to consent to cross-service data processing, in particular with a view to the number of clicks required;
- c. Ensuring that consent is not set as the default option; and
- d. Not offering a service at a lower quality to Users who decline to consent, unless the reduction in quality is a direct consequence of Google's inability to process Personal Data across services.

7. Google will provide Users a transparent, easily accessible and simple way to withdraw consent to cross-service data processing.

Accessibility

- Privacy choices should be accessible to all, including users with disabilities
- Readability: using clear and plain language helps everyone!
- Occasionally conflicting requirements
 - E.g. WCAG 2.1 focus order: “...a dialog opens and focus is set to the first interactive element in the dialog...”
 - -> Influences the user’s choice

Configure audit logging

Audit Log
Audit historical actions, such as request creation, request approval, and policy creation.

Search

<input type="checkbox"/>	User ↕	User identifier ↕
<input type="checkbox"/>	Jane Doe	erica.smith@email.com
<input type="checkbox"/>	Joe Bloggs	erica.smith@email.com
<input type="checkbox"/>	Jane Doe	an.employee@easytravel.com
<input type="checkbox"/>	Kathleen (Privacy Counsel)	a.customer@email.com
<input type="checkbox"/>	Maria (Privacy Analyst)	john.smith@email.com

This app writes audit logs for request and policy changes. There are a few important things you should know before you get started:

- Request audit logs contain sensitive data (the user identifier).
- By default, audit logs are ingested to the `default_logs` bucket.
- Alternatively, you can configure ingestion to a custom bucket to apply a custom retention period or access control.

The audit logging configuration will apply for all users on this tenant and can be changed later on.

☐ Use the default logs bucket

☐ Learn how to configure a custom bucket

Accessibility

- Is your cookie dialog navigable using a screen reader?
- Would a user even know it exists? (Consent!)

Screen readers and cookie consents

May 12, 2020 | @LDNWebPerf | ldnwebperf.org



Léonie Watson
@LeonieWatson



Let's talk about your privacy challenges!



Bonus: Forrester's Five Privacy Personas

Reckless Rebels

Very willing to share personal data. Most likely to share location data if they get something in return.

Conditional Consumerists

Use ad blockers, but are happy to share data if there's an incentive, like loyalty program perks

Data-Savvy Digitals

Understand how their personal data is (ab)used online and share it only when they have to.

Nervous Unawares

Unwilling to share personal data. Want to protect themselves online, but are unsure how to

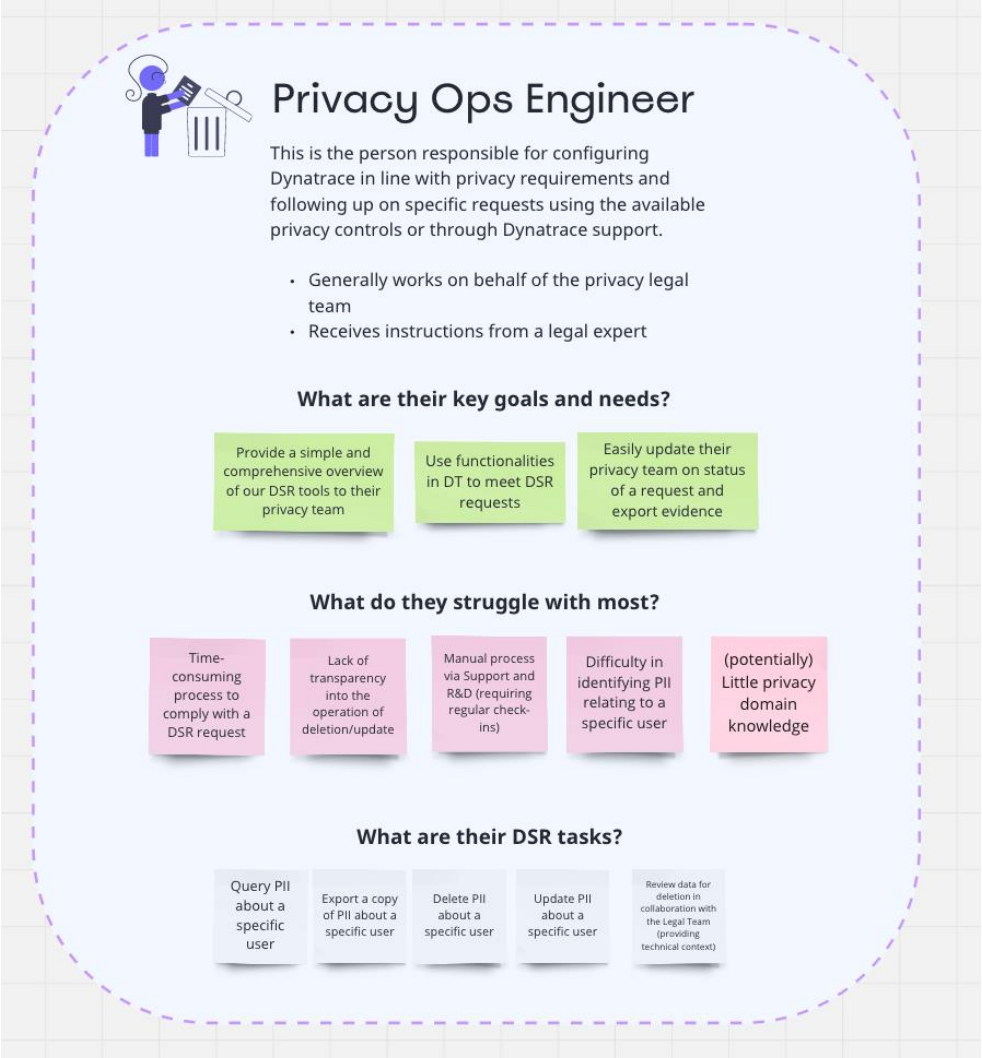


Sources: [1](#), [2](#)

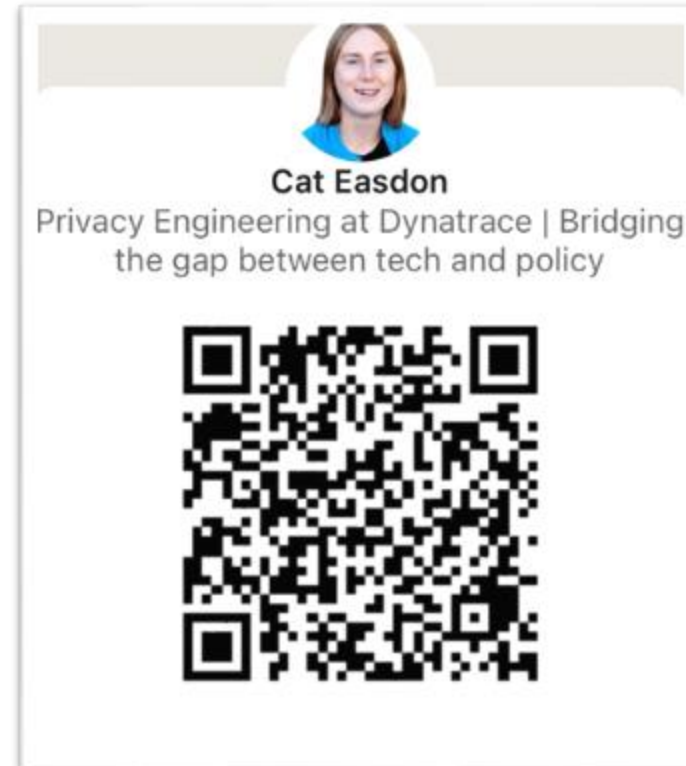
Skeptical Protectionists

The oldest user segment; unwilling to share personal data and trust few companies.

Bonus: The Privacy Ops Persona



Thanks for listening!



Copyright Notice

- **Dynatrace content and branding:** © 2024 Dynatrace LLC
- **Third-party images, text, and videos:** see links for attribution
- **Unattributed images:** generated with [DALL·E 3](#) or used under license from the [Noun Project](#)
- **All other content:** original work by the author, may be reused with attribution