

Privacy Architecture

Engin Bozdag
IN4315 - TU Delft 2022

Uber



Background

Experience

Principal Privacy Architect



Privacy Architect



Consultant &
Software
Engineer



Education

Computer Science (MSc, BSc)



Privacy & AI Ethics (PhD)



PERFORMANCE TESTING OF DATA DELIVERY TECHNIQUES FOR AJAX APPLICATIONS

ENGIN BOZDAG

Software Engineering Research Group, Delft University of Technology Mekelweg 4, 2628CD Delft, The Netherlands



ALI MESHAH

Software Engineering Research Group, Delft University of Technology Mekelweg 4, 2628CD Delft, The Netherlands

ARIE van DEURSEN

Software Engineering Research Group, Delft University of Technology & CWI Mekelweg 4, 2628CD Delft, The Netherlands

Keywords: Performance testing, Ajax, Web data delivery, Comet, Push/pull, Empirical study

An Adaptive Push/Pull Algorithm for AJAX Applications

Engin Bozdag, Arie van Deursen
Delft University of Technology
Mekelweg 4, 2628CD Delft, The Netherlands
{e.v.bozdag, Arie.vanDeursen}@tudelft.nl

Published
2009-09-16

Issue
2009: Vol 8 Iss 4

Section
Articles

Agenda

01 Introduction

02 Privacy

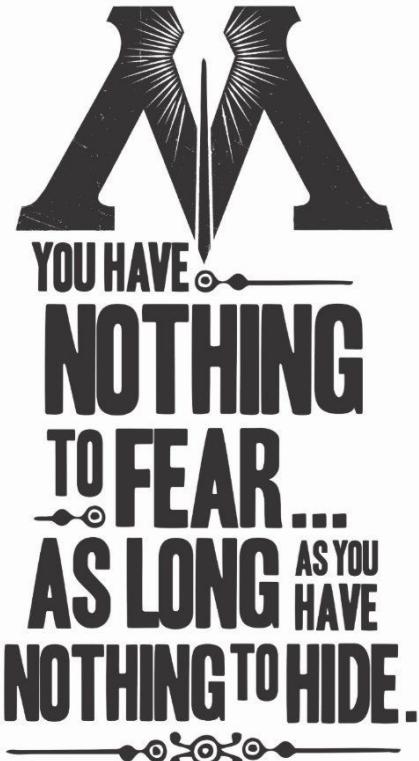
03 Privacy Engineering

04 Dark Patterns

05 Q & A

Privacy

Why Privacy?



TM & © Warner Bros. Entertainment Inc.

(s10)



The Belastingdienst logo on a window - Credit: [Joepoulsen / Depositphotos](#) - License: [DepositPhotos](#)

Tax office fined €2.75 million for privacy violations in benefits scandal

UK Police's Facial Recognition Systems Are Wrong Up To 98% Of The Time

By [Lucian Armasu](#) published May 15, 2018

A face-scanning algorithm increasingly decides whether you deserve the job

Amazon scraps secret AI recruiting tool that showed bias against women

APRIL 14, 2020



Half of Americans have decided not to use a product or service because of privacy concerns



“Seventy-one percent said they would stop doing business with a company if it gave away sensitive data without permission.”

What is Privacy?

Privacy is about security of personal data

Privacy is protecting sensitive data

Privacy is GDPR

Privacy is only for lawyers

Privacy is about selling data

Privacy Is not Security

- Security => confidentiality, availability and integrity of any (sensitive) data
- Privacy needs security, but more
 - Example: Best encryption algorithm + strict access control
 - Not enough for privacy

Privacy Principles



All data needs to expire



Minimize what you collect & de-identify



Privacy Rights: Delete, Access (Export), Correct, etc.



Purpose Limitation



Consent

Give user control



Transparency & Respect

Personal Data

What is personal data?



COLLECT
STORE
USE
DATA?

You have to abide
by the rules.

Direct Identifiers:

- Name
- Phone number
- Address

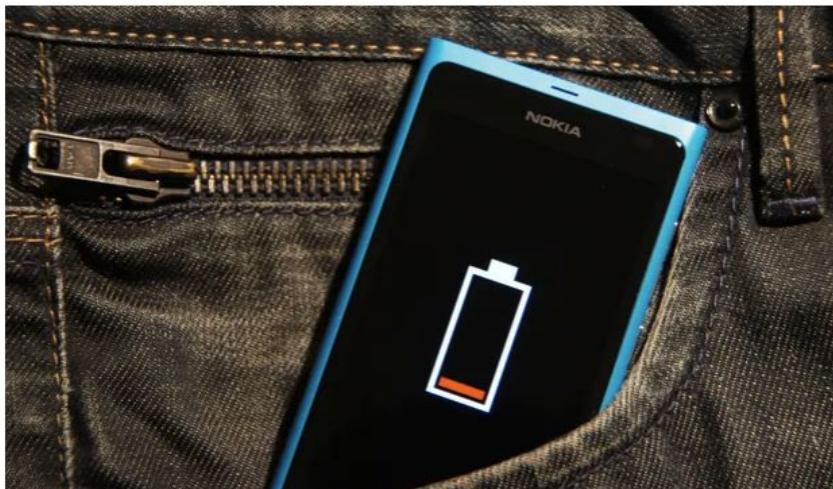
Indirect Identifiers:

- User UUID
- Battery Level,
- Advertising ID (e.g. Apple IDFA)
- Trips, Logs, Battery Level, etc.

Personal Data: Linkability Risks

Your battery status is being used to track you online

Battery status indicators are being used to track devices, say researchers from Princeton University - meaning warnings of privacy exposure have come to pass



Battery API

- the current level of battery (format: 0.00-1.0, for empty and full, respectively)
- time to a full discharge of battery (in seconds)
- time to a full charge of battery, if connected to a charger (in seconds)

Personal Data or Not?

Quiz

Which of these six datasets is classified as **Personal Data**

Vehicle color,
vehicle make

Vehicle color,
vehicle make,
postal code

Location data
(>2 decimal
points)

IP Address

Drop-off or
pick-up
location

First or last
name



Personal Data or Not?

Quiz

Which of these six datasets is classified as **Personal Data**

Vehicle color,
vehicle make



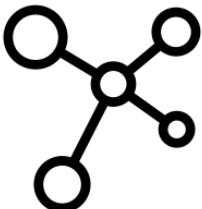
Vehicle color,
vehicle make,
postal code

Location data
(>3 decimal
points)

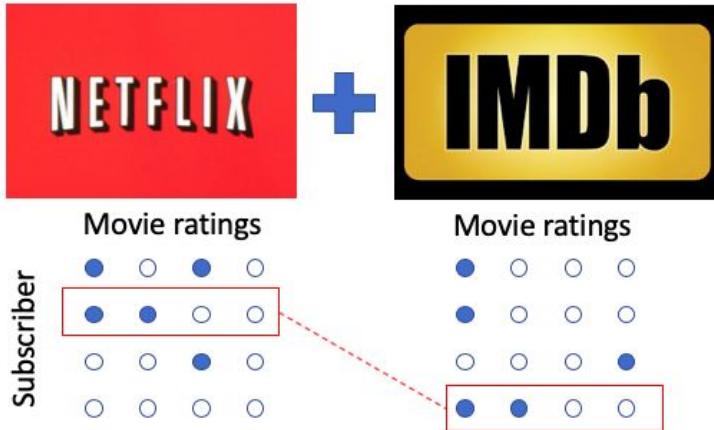
IP Address

Drop-off or
pick-up
location

First or last
name



Personal Data: Linkability Risks



NYC Taxi Data Blunder Reveals Which Celebs Don't Tip—And Who Frequents Strip Clubs

By cross-referencing de-anonymized trip data with paparazzi photos, a privacy research could tell how much Bradley Cooper paid his driver.



Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims

An in-the-closet lesbian mother is suing Netflix for privacy invasion, alleging the movie rental company made it possible for her to be outed when it disclosed insufficiently anonymous information about nearly half-a-million customers as part of its \$1 million contest to improve its recommendation system. The suit known as Doe v. Netflix (.pdf) was filed [...]

NetFlix Cancels Recommendation Contest After Privacy Lawsuit

Netflix is canceling its second \$1 million Netflix Prize to settle a legal challenge that it breached customer privacy as part of the first

Privacy Engineering

Deletability

- Two use cases:
 - Delete when no longer needed (TTL)
 - Delete when user deletes their account

Deletability

- Can the system hard delete the data in a scalable manner?
 - Cassandra & soft delete

```
CREATE TABLE  
device_measurements (  
    device_id uuid,  
    measurement_type text,  
    measurement_value text,  
    user_id uuid,  
    PRIMARY KEY (device_id,  
    measurement_type));
```

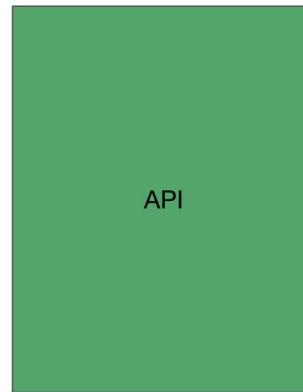
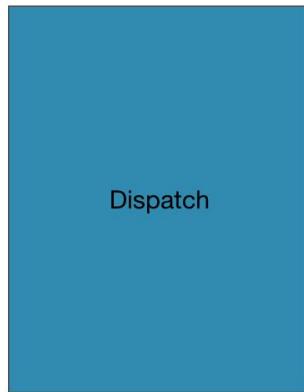
```
DELETE FROM device_measurement WHERE  
user_id = bf884b98-0a72-10e8-ba89-0ed5f89f718b
```

```
DELETE FROM  
device_measurement WHERE  
user_id =  
bf884b98-0a72-10e8-ba89-0ed5f8  
9f718b ALLOW FILTERING
```

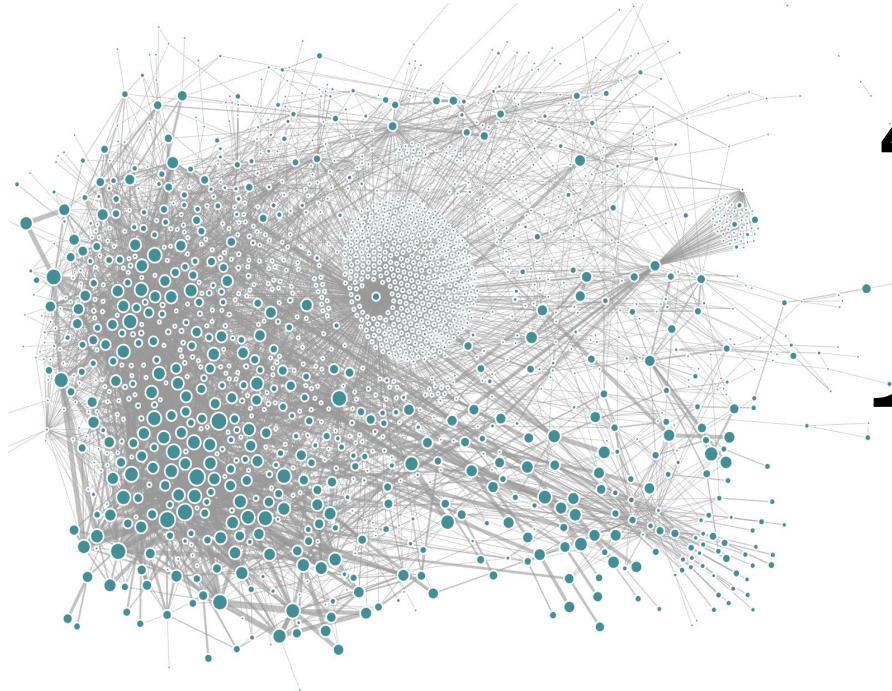
Deletability

- Can you locate all of the user's personal data?
 - Based on a userUUID/email?
 - Are all data tagged?
- Should you delete that data?
 - Safety / Fraud detection
 - Tax law
 - Log files for security
- Also applies to export

Uber Architecture 1.0 (2011 - 2015)



Uber Architecture 2.0 (2015- present)



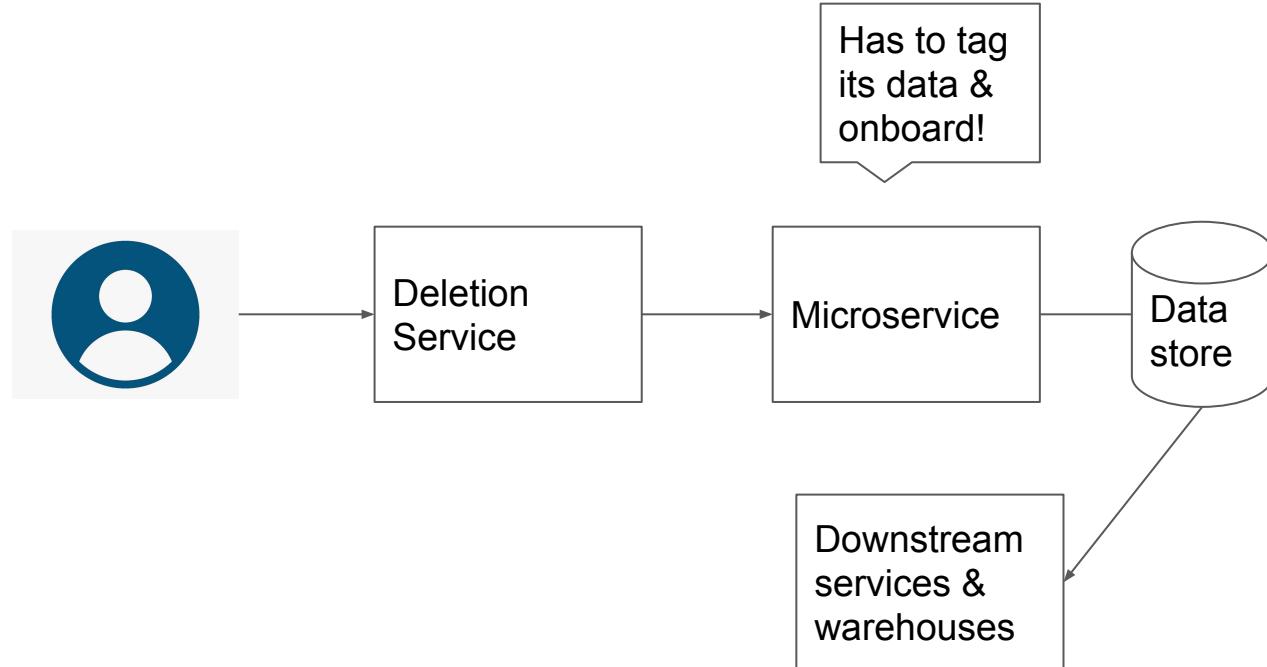
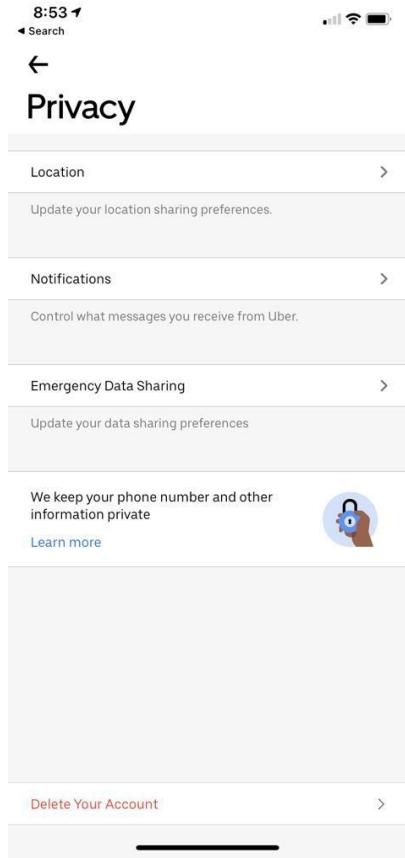
4000+
Microservices

100M+
Users

50+
Apps

71
Countries

Deletion Orchestrator



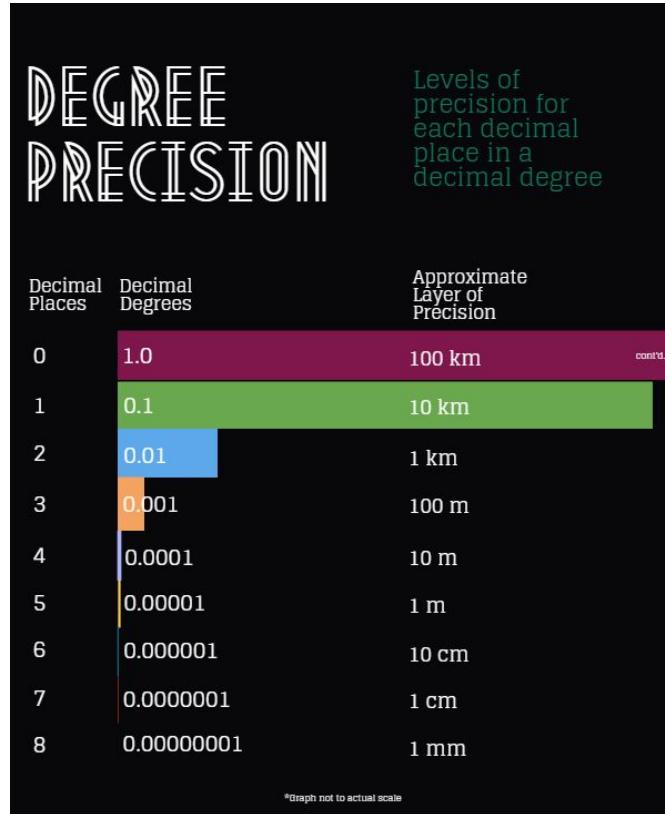
Minimize Collection

- Do I need to collect this data?

The screenshot shows a mobile application's sign-up interface. At the top, there is a header bar with signal strength, network name 'T-Mobile NL', battery level at 87%, and the time 21:06. Below the header is a button labeled 'JOIN'. The main form area starts with a placeholder 'john' in a text input field, followed by 'doe' in another. There is a circular profile picture placeholder with a camera icon and a plus sign. Below the names are gender selection buttons: 'Male' (selected) and 'Female'. A prominent error message 'Please provide your gender' is displayed over the email input field, which contains 'test@telenet.be'. The password field is filled with '*****'. The birthdate is listed as '25 January 1972'. At the bottom, a note states: 'By continuing you accept our Terms of Service & Privacy Policy.'

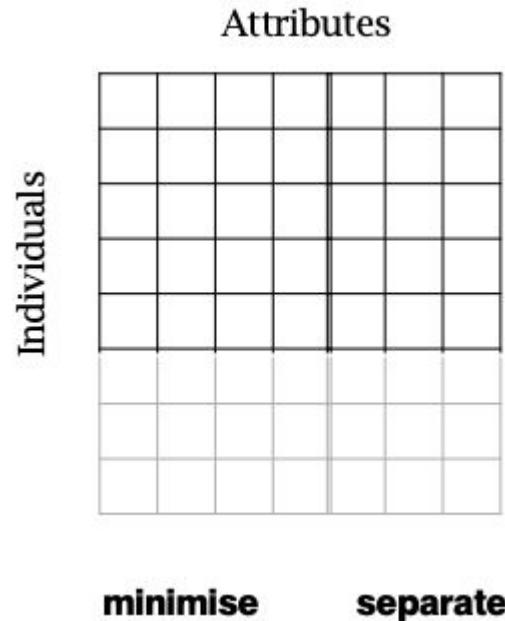
Minimize Granularity & Abstract

- Do I need precision for my purpose?
- Can I remove some columns, add noise, aggregate?



Separate

- Do I need identifiability for analytics?
 - User's email
 - Phone nr
 - userUUID / linkable data
- Do not dump everything into one db
 - use different tables/db's
 - Different granularity (safety vs analytics)
 - Different access controls



Hide

- Did you categorize sensitive/confidential/public data?
- Do you encrypt sensitive data at rest?
 - Do you use a state of the art method?
 - Do you rotate your keys?
- Tensions: performance



Dark Patterns

Dark Patterns

“a user interface that has been carefully crafted to trick users into doing things”

“Ways to manipulate or sway consumers in a certain direction”

[Unsubscribe](#)



Confirmshaming

• • •



Want to help your dog by signing up for our newsletter?

Yes, gladly

I don't want to help my dog

Enter your email + enjoy

15% OFF

YOUR ENTIRE ORDER

"Hooray!" said your home.

Enter your email address

get my 15%

No thanks, I'm not into savings >

Get the best recipes in your inbox

Email address

LET'S COOK

No, I prefer canned soup

SPOON
UNIVERSITY

Bait and Switch

The screenshot shows a Windows 10 setup window titled "Get Windows 10". In the top right corner, there is a link to "Learn more on windows.com". The main content area has a heading "Manage your settings for face recognition". Below it, a sub-section titled "Face recognition" explains how the system compares user photos with tagged photos and videos. Two radio button options are shown: "Allow Facebook to recognise me in photos and videos" and "Don't allow Facebook to recognise me in photos and videos". The second option is highlighted with an orange border. At the bottom, there are three buttons: "MANAGE DATA SETTINGS" (highlighted with an orange border), "ACCEPT AND CONTINUE" (highlighted with an orange border), and "CONTINUE".

Turn on face recognition if you want us to use this technology

If you turn this setting on, we'll use face recognition technology to understand when you might appear in photos, videos and the camera to do things such as help protect you from strangers using your photo, find and show you photos that you're in but haven't been tagged in, tell people with visual impairments who's in a photo or video, and suggest people that you may want to tag. Select Accept and Continue to turn on face recognition or Manage Data Settings to keep it turned off.

What's collected?

UPD

Manage your settings for face recognition

Face recognition

Before you manage your data settings, these examples can help you decide what choices to make.

💡 Face recognition technology allows us to help protect you from a stranger using your photo to impersonate you or tell people with visual impairments who's in a photo or video using a screen reader.

💡 If you keep face recognition turned off, we won't be able to use this technology if a stranger uses your photo to impersonate you. If someone uses a screen reader, they won't be told when you're in a photo unless you're tagged.

Allow Facebook to recognise me in photos and videos

Don't allow Facebook to recognise me in photos and videos

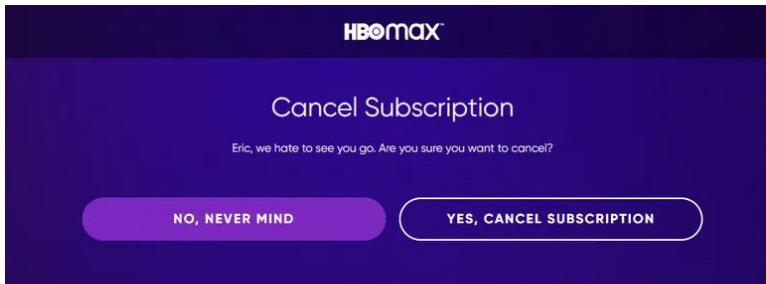
MANAGE DATA SETTINGS

ACCEPT AND CONTINUE

CONTINUE

Skip

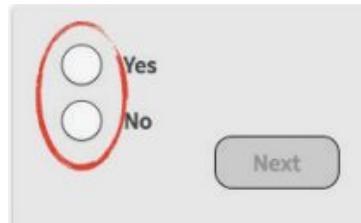
Bait and Switch



Drives Opt-In

Yes
 No

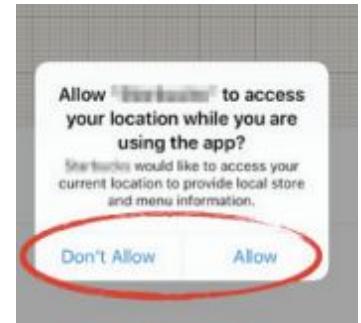
[Next](#)



Drives Opt-Out

Yes
 No

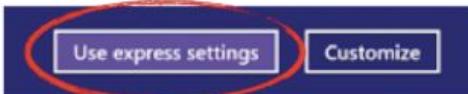
[Next](#)



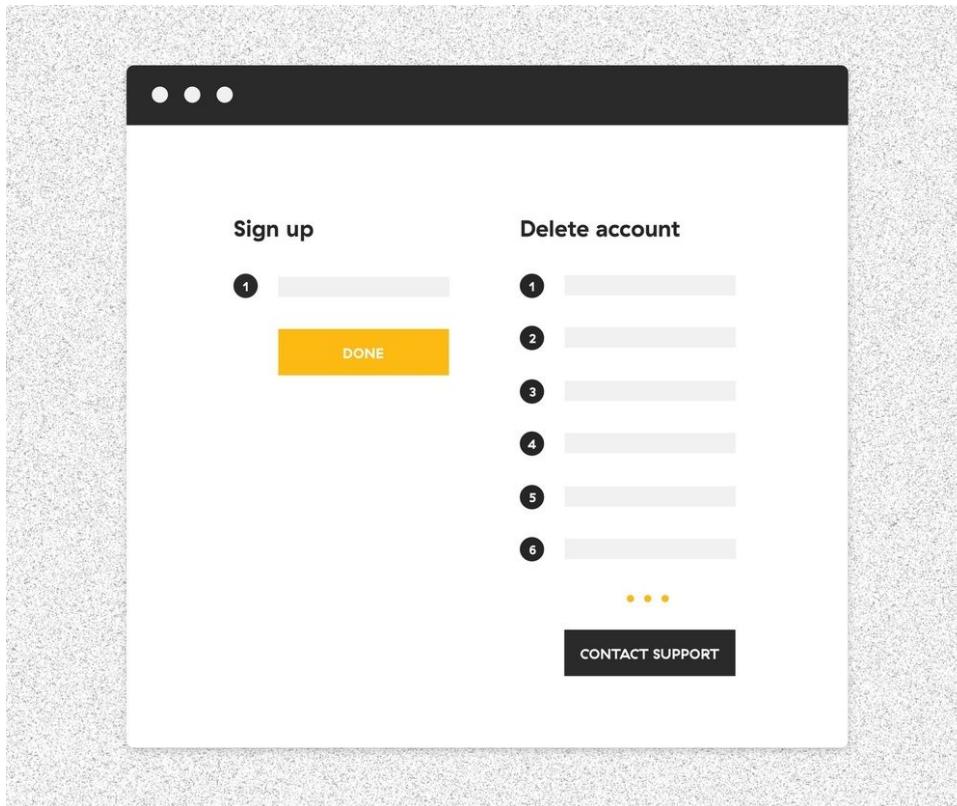
Drives a Decision

Yes
 No

[Next](#)



Roach Motel



Your Amazon.com Inquiry

Inbox  Amazon 



cs-reply@amazon.com

to me 

7:21 PM (0 minutes ago)



Hello,

I want to make sure that closing your Amazon.com account and deleting your data won't cause problems with any open transactions or other websites you might visit.

You won't be able to access your account once it's closed, and you won't be able to reopen it. You won't be able to access your order history, initiate a return, or print a proof of purchase or invoice. Please ensure you retain all proof of purchase, which may be applicable for any warranties. All open orders, including subscriptions (Amazon Prime, Subscribe and Save, etc.), will also be canceled.

You will no longer have access to:

- Your Amazon.com account and all Amazon accounts worldwide.
- Your Amazon.com Associates, Seller, Partner Program, Amazon Flex, Author Central, Kindle Direct Publishing and Mechanical Turk accounts.
- Your Amazon Web Services (AWS) account. Any content and AWS resources will be terminated and cannot be restored.
- Your customer profile, including your reviews, discussion posts, and customer images.
- Digital content and subscriptions related to Kindle, Prime Video, Amazon Music, Amazon Drive, Prime Photos, and your Amazon Appstore purchases.
- Any outstanding Gift Card or promotional credit balances.
- Your Textbook Rental returns. You will remain responsible for any outstanding rentals.
- Your Amazon Pay account.
- Your Audible.com account and audio books from Audible.com.
- Your Lists and Registries, if applicable, or About You page.

You will permanently lose access to any Amazon Drive or Prime Photos content once your account is closed. We suggest you download and save any content before closing your account.

You may need to deregister devices or apps before your account is closed. You can deregister these through the Manage Your Content and Devices page (<https://www.amazon.com/mycd>).

Your internet browser may have stored additional information about your Amazon account. You can delete your browser's cookies through your browser settings; this will remove all information stored on your browser.

If you have an Amazon Web Services account, please contact AWS customer support for assistance with closing your AWS account:

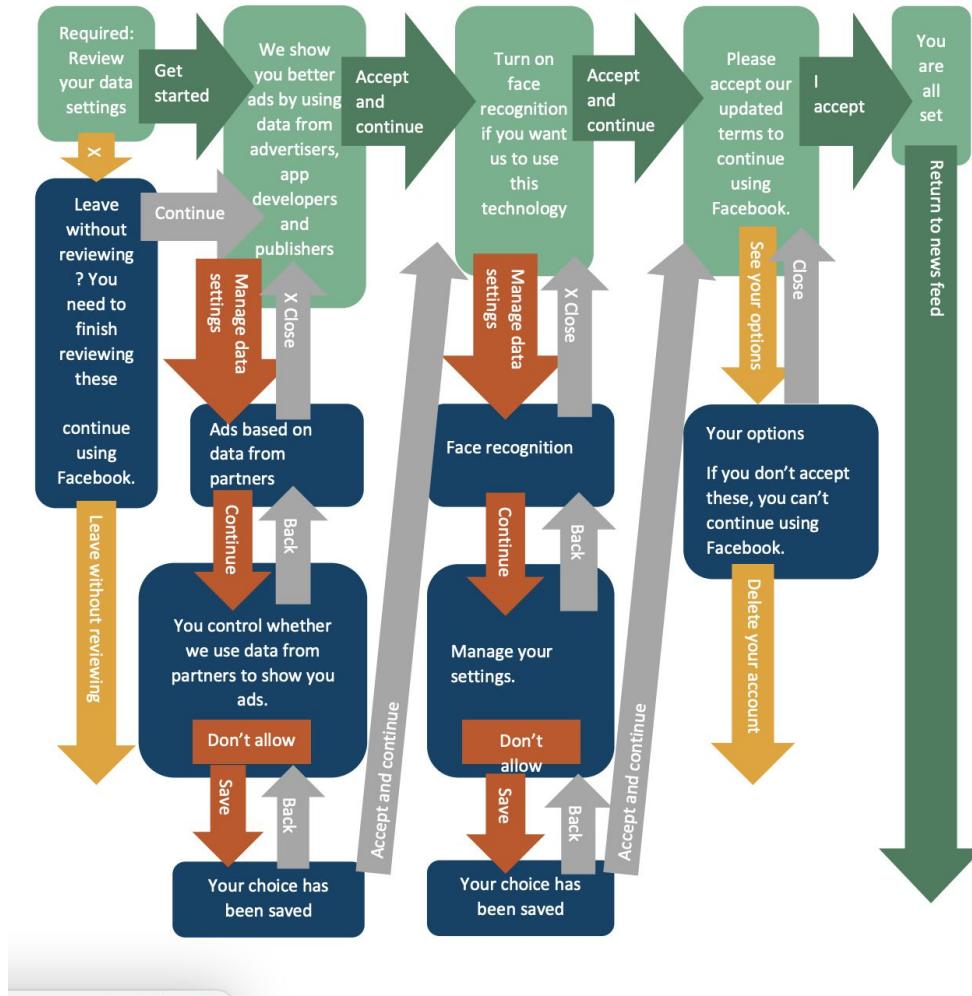
<https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/aws-account-and-billing>

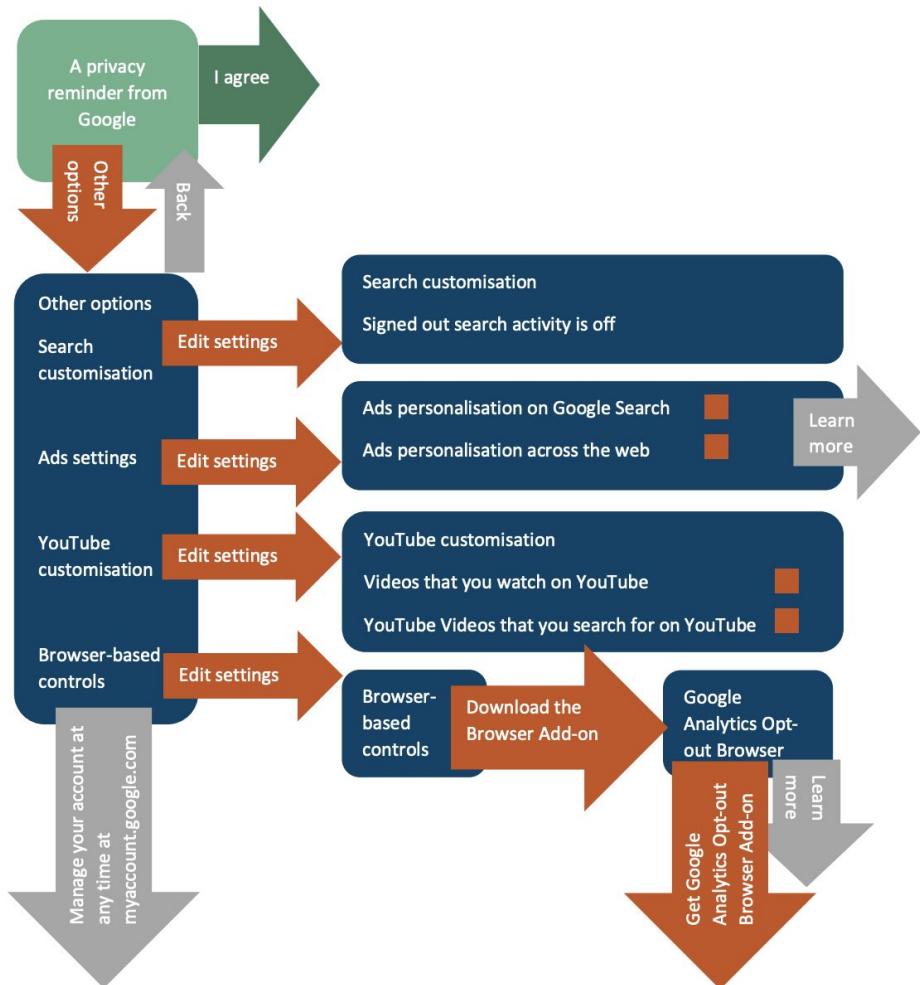
If you have a Kindle Direct Publishing (KDP) account, please contact KDP customer service for assistance with closing your KDP account:

<https://kdp.amazon.com/self-publishing/contact-us>

If you still want to close your Amazon.com account after reviewing the items above, please click this link and state that you want to close your account:

<https://www.amazon.com/gp/help/rsvp/rsvp-mi.html?q=acc1>





Privacy Zuckering

The image consists of three screenshots from mobile devices, likely an iPhone, demonstrating privacy changes.

Screenshot 1: WhatsApp Privacy Settings

This screenshot shows the WhatsApp "Privacy settings" screen. It includes sections for "Check a few important settings", "Manage your profile", and "Learn more with Privacy Basics". Below these are sections for "YOUR ACTIVITY" and "HOW PEOPLE CAN FIND AND CONTACT YOU". A red circle highlights the "Who can see your future posts?" section under "YOUR ACTIVITY", which is set to "Public".

Screenshot 2: WhatsApp Terms and Privacy Policy Update

This screenshot shows the WhatsApp update to its Terms and Privacy Policy. It features a circular graphic with various icons. The text explains the update to reflect new features like WhatsApp Calling and provides links to the Terms and Privacy Policy. At the bottom, there is an "Agree" button and a link to read more about key updates.

Screenshot 3: Facebook To Do Feed

This screenshot shows the Facebook "To Do" feed at 9:00 AM. It displays news items from Lisa Huffonton, Marissabel Fernandez, and Alicia Han. The feed also includes a "Congratulate" button for Marissabel Fernandez's job update and a "Tell Your Network" button for Alicia Han's news mention. The top of the screen shows a navigation bar with "Privacy settings" and other icons.

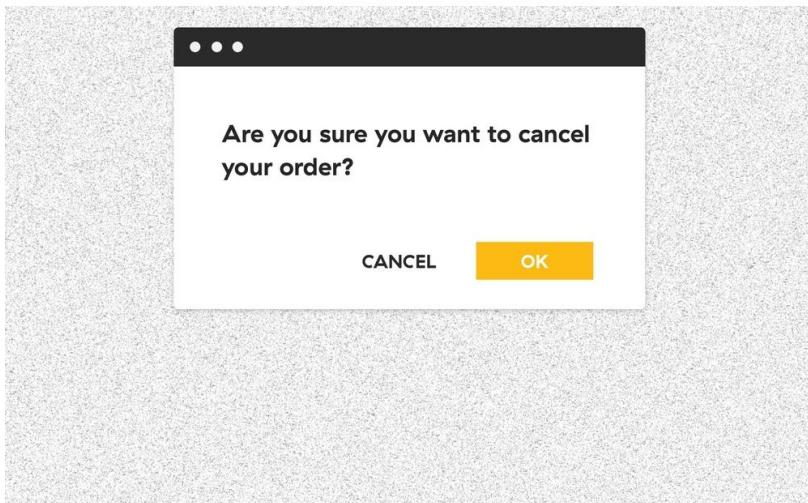
Trick Questions

WIRED and Conde Nast would like to contact you with offers and opportunities. Please tick here if you would prefer to receive these messages: by email by sms

If you do not wish to hear from us about other relevant offers please tick here: by post by phone

Our partners sometimes have special offers that we think you will find relevant, please tick here if you would prefer to receive these messages: by email by sms

Please tick here if you would prefer not to hear from our partners: by post by phone



Dark Patterns - what can you do?

- Be aware of cognitive biases
- Ask companies details about your data
- Do not use them when building your product

Google Illegally Used Dark Patterns to Trick Users Into Handing Over Location Data, State AGs Say

The D.C. and Texas lawsuits allege the "deceptive and unfair" practices may have violated local laws.

By Mack DeGeurin | Monday 10:55AM | Comments (11) | Alerts

Dark Patterns: EU countries want to ban psychological tricks with the Digital Services Act

France cracks down on dark patterns, fining Google and Facebook nearly \$240 million for manipulative cookie tricks

BY DAVID MEYER

January 6, 2022 9:21 AM CST

Conclusion

- Design for deletability and exportability
- Know where user data is and tag it
- Minimize collection and aggregate
- Separate and hide
- Properly anonymize data before making it public
- Do not use dark patterns

Questions?

Appendix

Interviewing at Uber

Software Engineer - Privacy

1. Coding: Algorithms & data structures
2. Coding: Depth in specialization/chosen technology (Distributed Systems, Mobile, ML, Data)
3. System Design
4. Behavioral (team-work, self-awareness, conflict handling)

Privacy Engineer

1. Privacy System Design
2. Privacy Domain Knowledge
3. Cross-Functional Work (Data, Legal, Security)
4. Behavioral (team-work, self-awareness, conflict handling)