DSC 291 Privacy-sensitive Data Systems (week 3a)

Haojian Jin

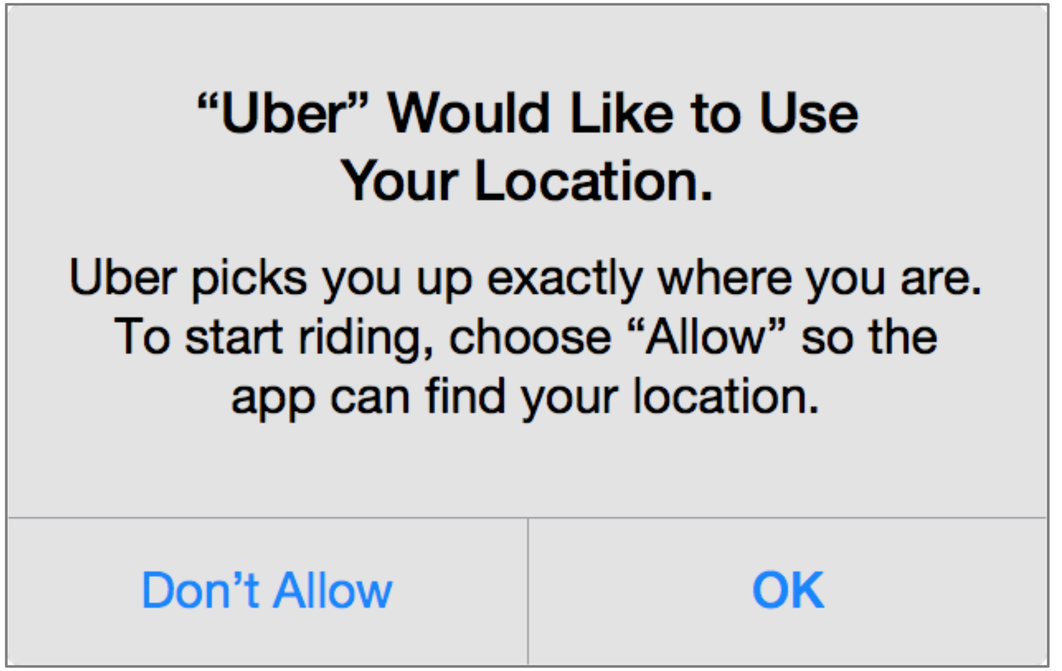
Logistics

1. New review format.
2. Discussions
    1. Presentations & Peer evaluation.
    2. Ask me anything.
3. Final project
    1. Abstract due Feb. 15.
    2. Final report due Mar. 19
4. Grades

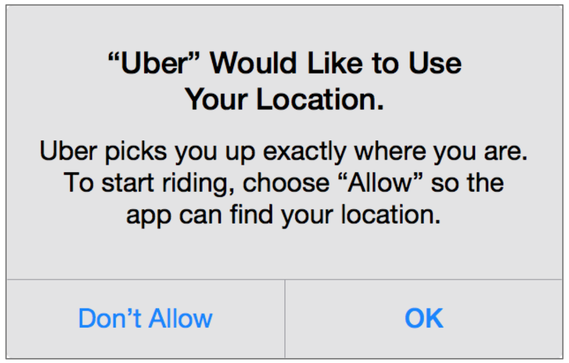
Recap: Location Privacy

- Why location privacy?
- Location-based applications
- Locating technologies
- Protecting location privacy
- Beyond location privacy
- Purpose framework
  - Data collection, data processing, data usages

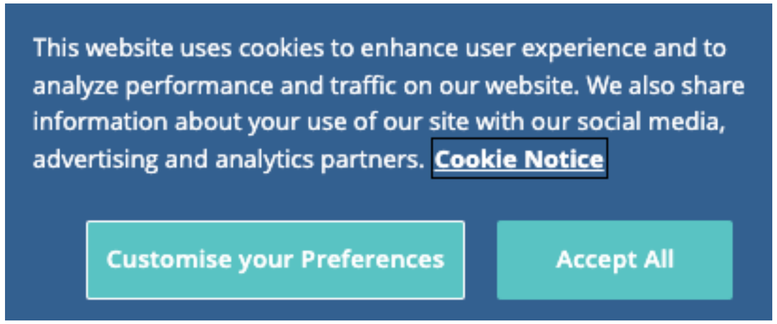
Todays' topic: Permissions



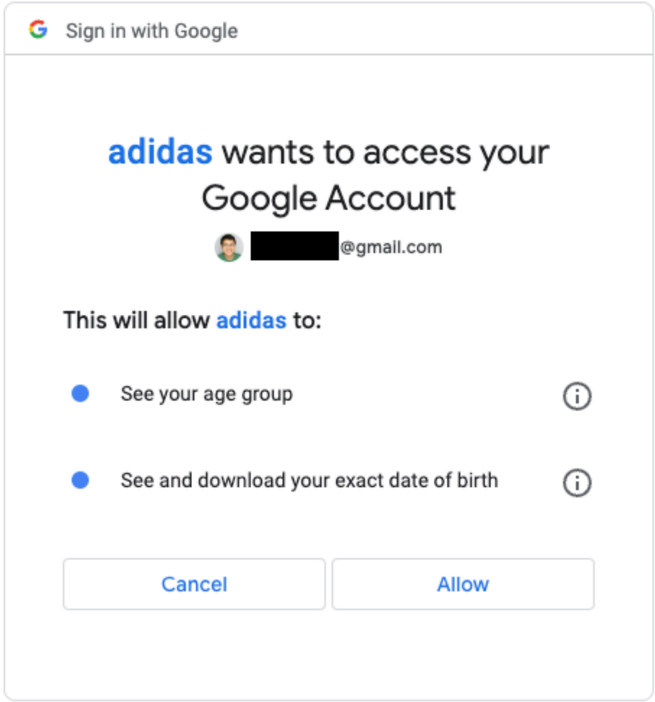
Three systems



Android permission

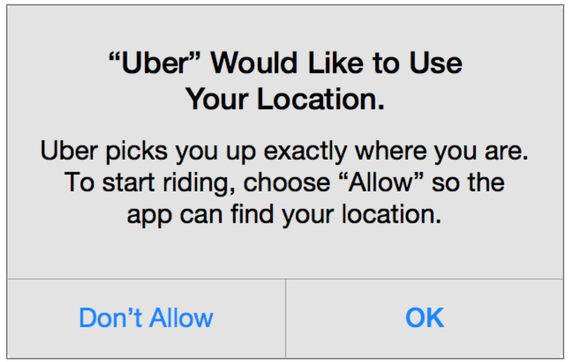


Browser cookie consent



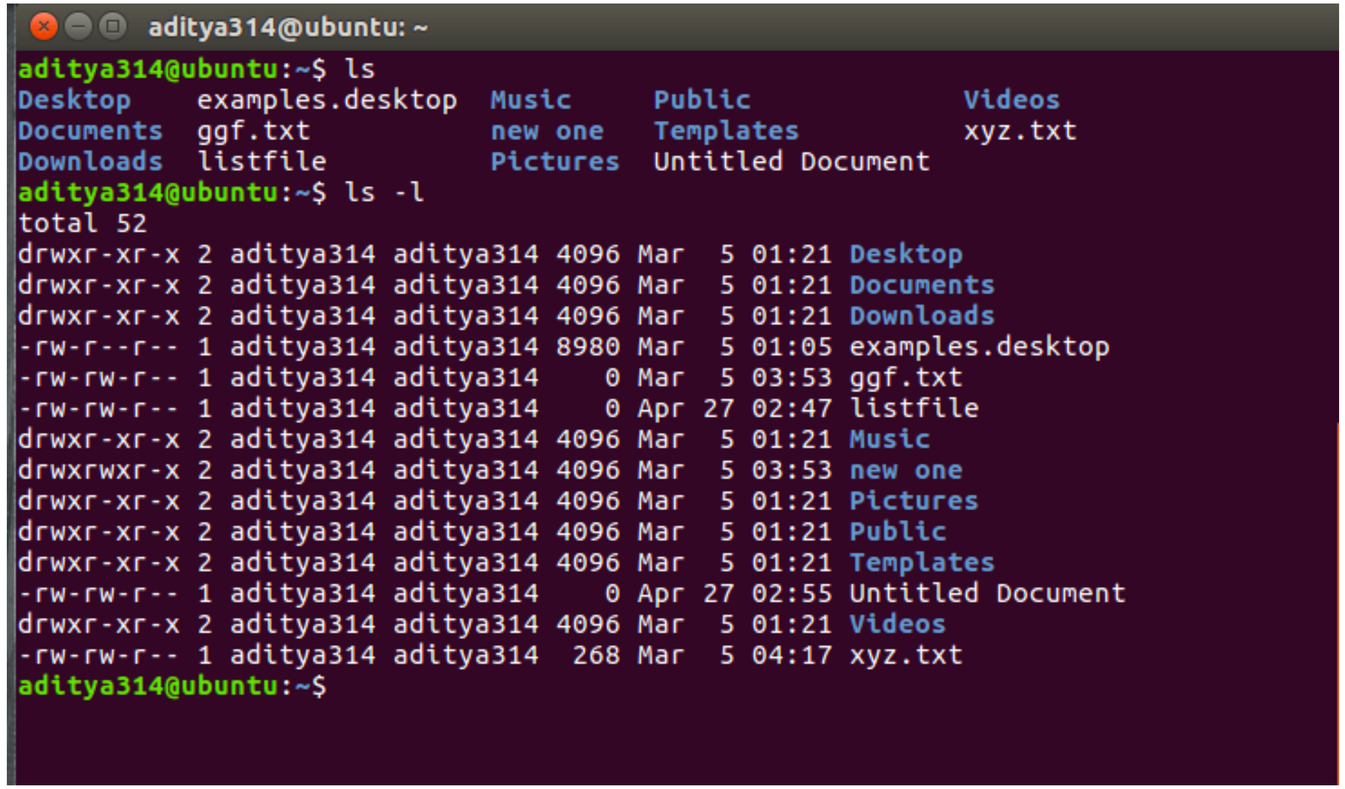
OAuth

Key privacy concepts



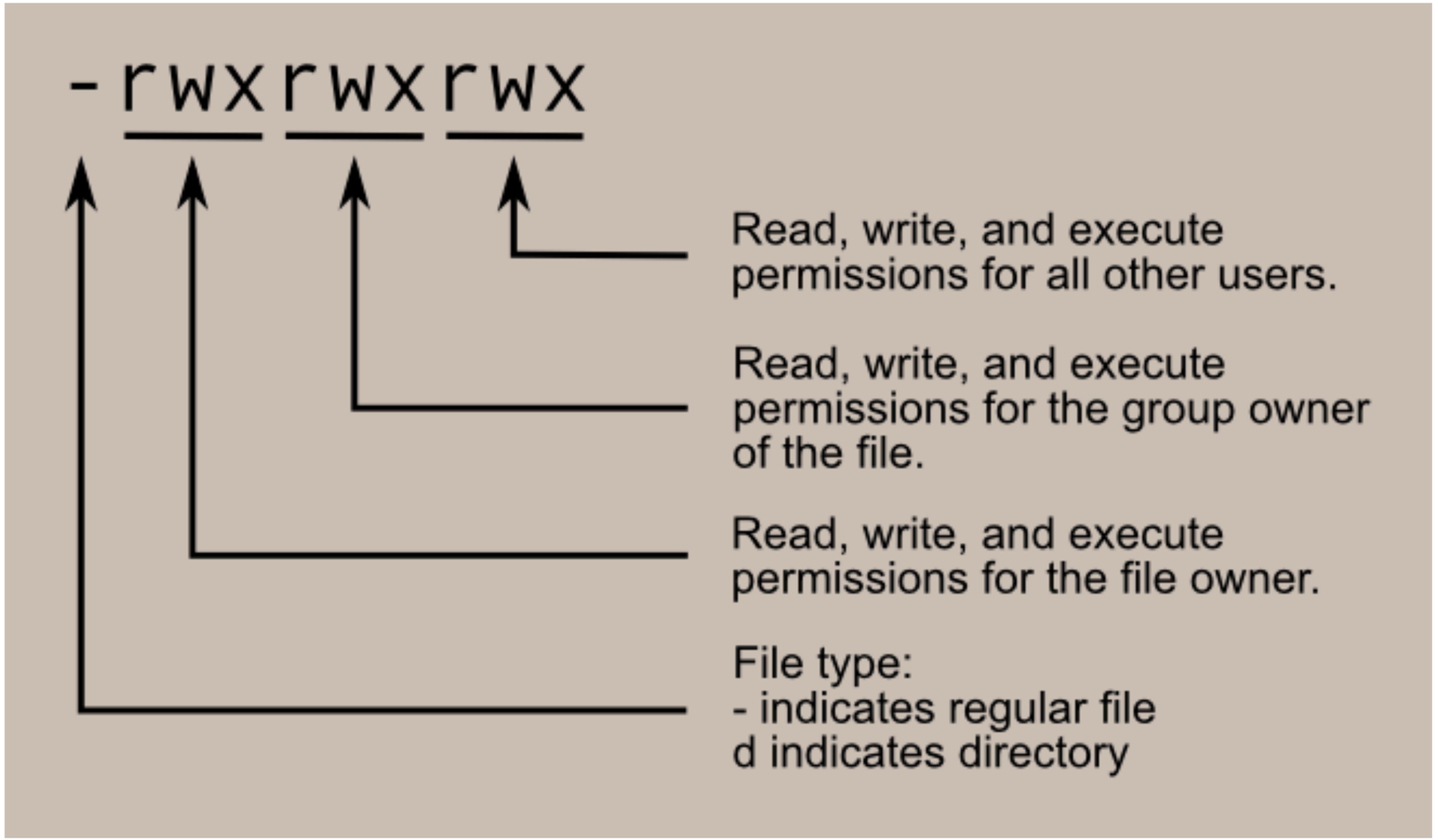
- Control
- Notice
- Consent
- Usability
- System mechanisms

Linux systems



- Users
- Permissions

File permissions



Why permissions?

- Notice
- Control
- Consent

Why permissions?

- Notice
  - Did users read the form?
  - Did users understand the form?
  - Can users understand the form?
  - Is the form accurate?

Why permissions?

- Control
  - Do they have a control?
  - Is it all-or-nothing?
  - Is it easy to control?
  - Do developers respect users' control?

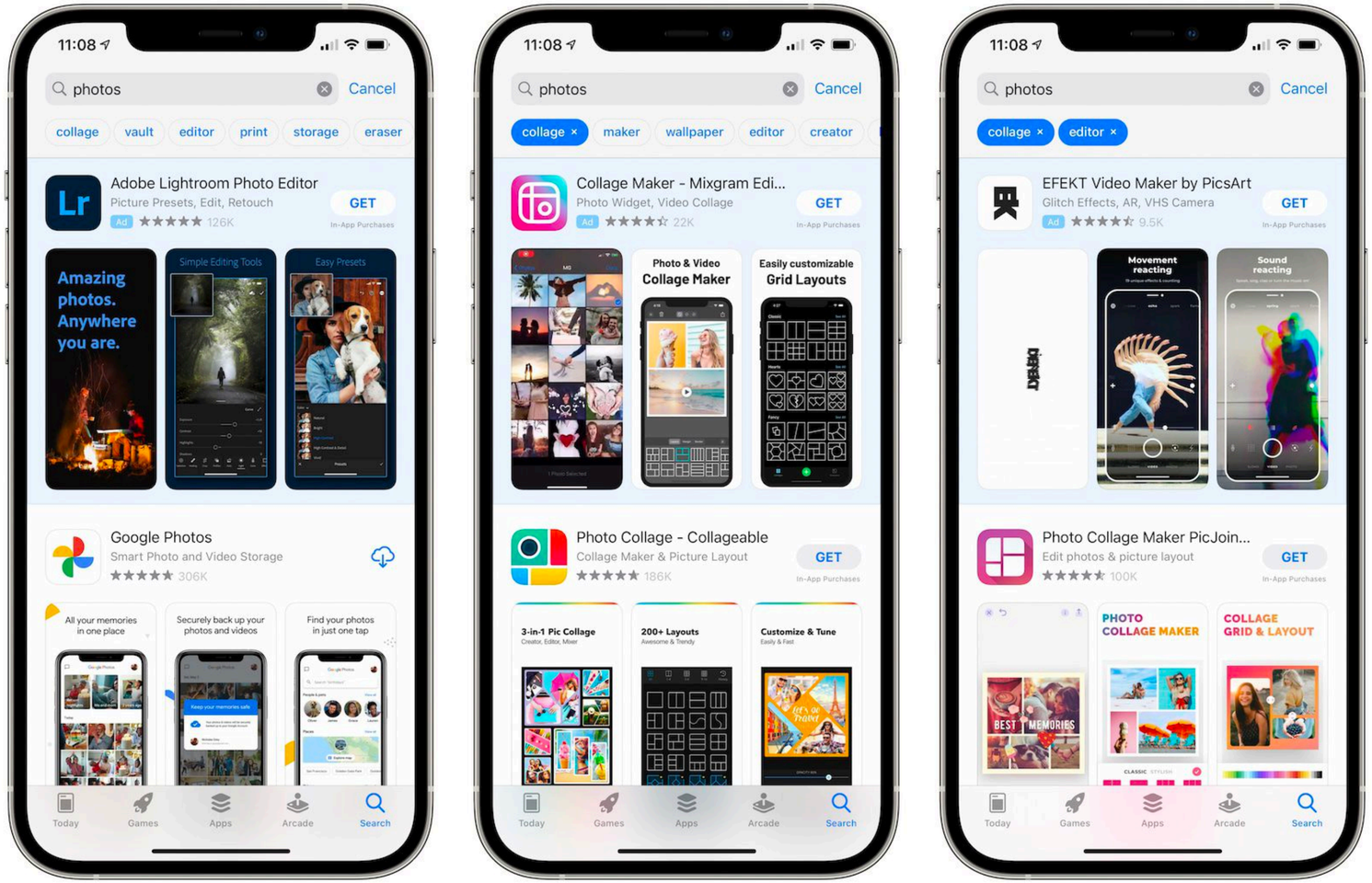
Why permissions?

- Consent
  - What's valid consent?
  - What if I agree to give up my privacy?
  - What if I leak other people's privacy?

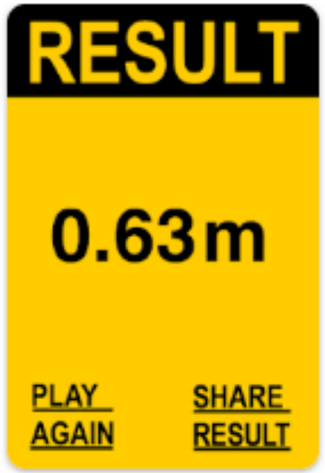
What works in med do not work in privacy.

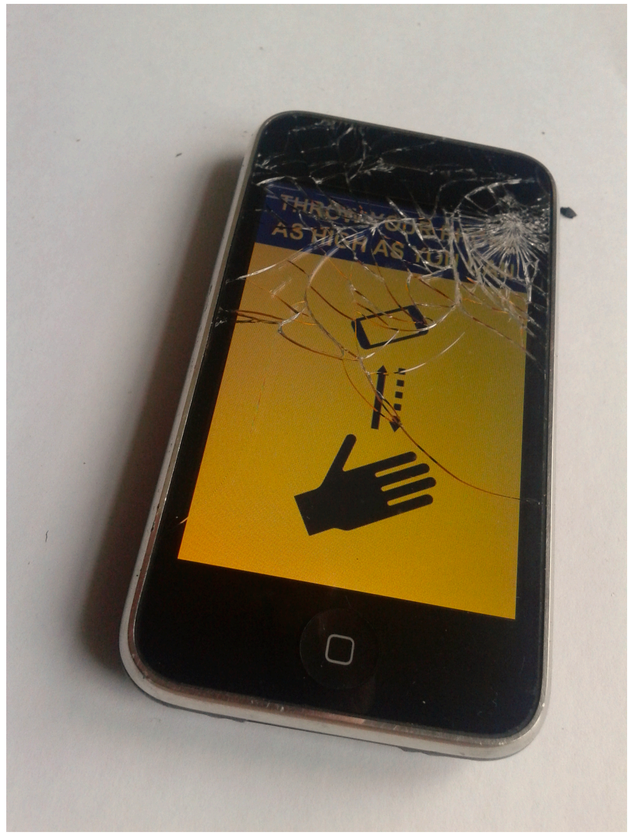
- Scale
  - Burdens on users
- Intangible data
  - Hard to enforce
- Motivations, awareness, knowledge
  - Less sensitive on long-term risks

App Store


11:08
photos
Cancel
collage
vault
editor
print
storage
eraser
Adobe Lightroom Photo Editor
Picture Presets, Edit, Retouch
Ad
126K
GET
In-App Purchases
Amazing photos. Anywhere you are.
Simple Editing Tools
Easy Presets
Google Photos
Smart Photo and Video Storage
306K
All your memories in one place
Securely back up your photos and videos
Find your photos in just one tap
Today
Games
Apps
Arcade
Search
11:08
photos
Cancel
collage
maker
wallpaper
editor
creator
Collage Maker - Mixgram Edi...
Photo Widget, Video Collage
Ad
22K
GET
In-App Purchases
Photo & Video Collage Maker
Easily customizable Grid Layouts
Photo Collage - Collageable
Collage Maker & Picture Layout
186K
GET
In-App Purchases
3-in-1 Pic Collage
200+ Layouts
Customize & Tune
Today
Games
Apps
Arcade
Search
11:08
photos
Cancel
collage
editor
EFEKT Video Maker by PicsArt
Glitch Effects, AR, VHS Camera
Ad
9.5K
GET
In-App Purchases
Movement reacting
Sound reacting
Photo Collage Maker PicJoin...
Edit photos & picture layout
100K
GET
In-App Purchases
PHOTO COLLAGE MAKER
COLLAGE GRID & LAYOUT
BEST MEMORIES
Today
Games
Apps
Arcade
Search

S.M.T.H.: Send Me to Heaven





100+ million => a few billion

- Putting apps in a sandbox & permissions.
  - Developers cannot ask/persuade/trick users for permissions to do dangerous thing.
- Better way to distribute software
- Centralized payments

How Android Applications work (1)

- Java source code → compiled into .dex byte-code file
- .dex file + Manifest file + resources = .apk archive
- Application isolation → **system level security**
  - Linux process, address space
  - VM (Dalvik Virtual Machine) for each application
  - unique Linux user ID
  - direct access only to its own data
  - API-based access to other apps' resources
- Not a single entry-point (no main)

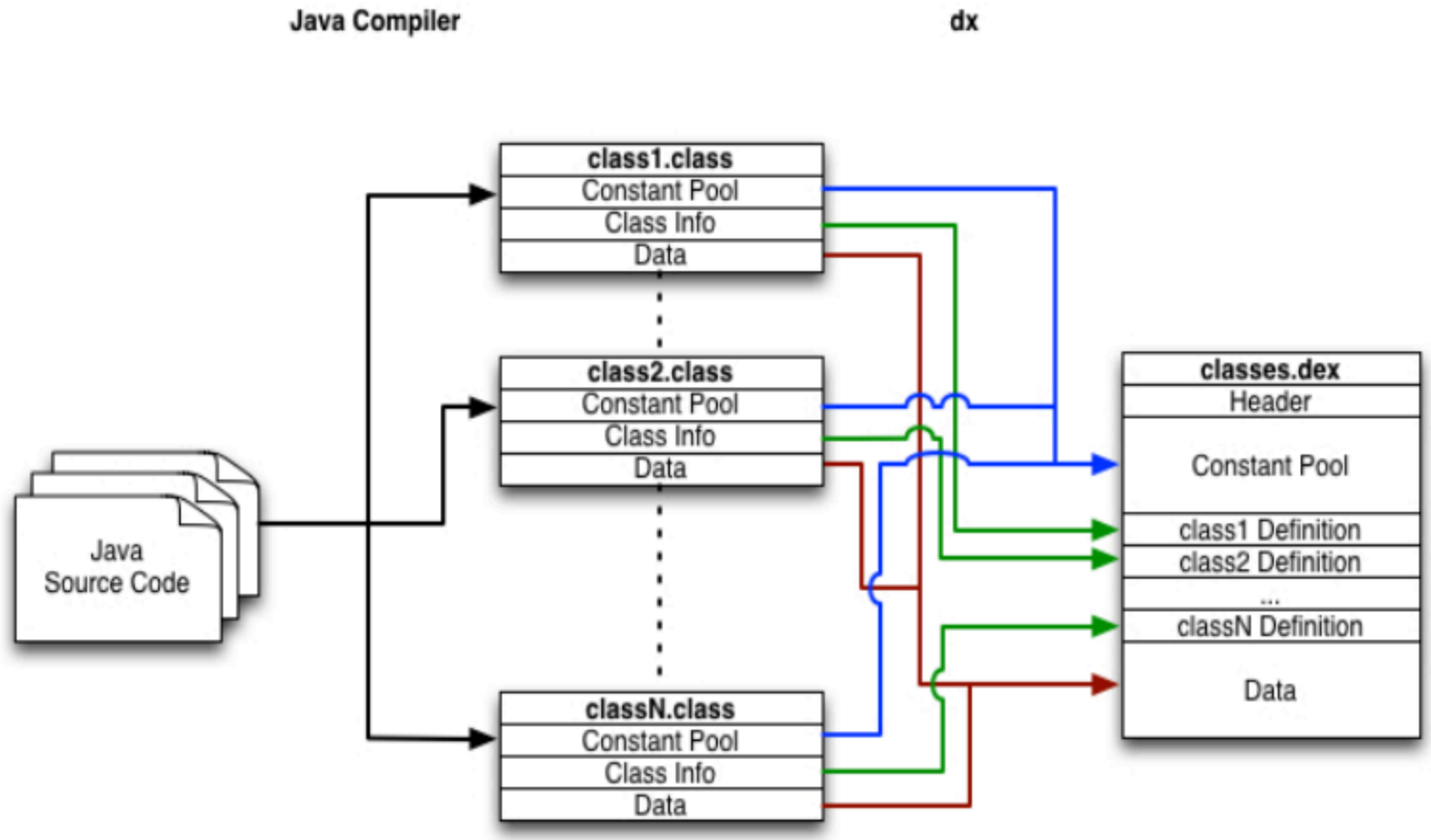
How Android Applications work (2)

- Applications can start each other
- Based on Components and Intents
- .dex - Dalvik Executable format
- Dalvik is optimised for mobile architectures
  - low memory consumption
  - Dex results in smaller binaries than JAR

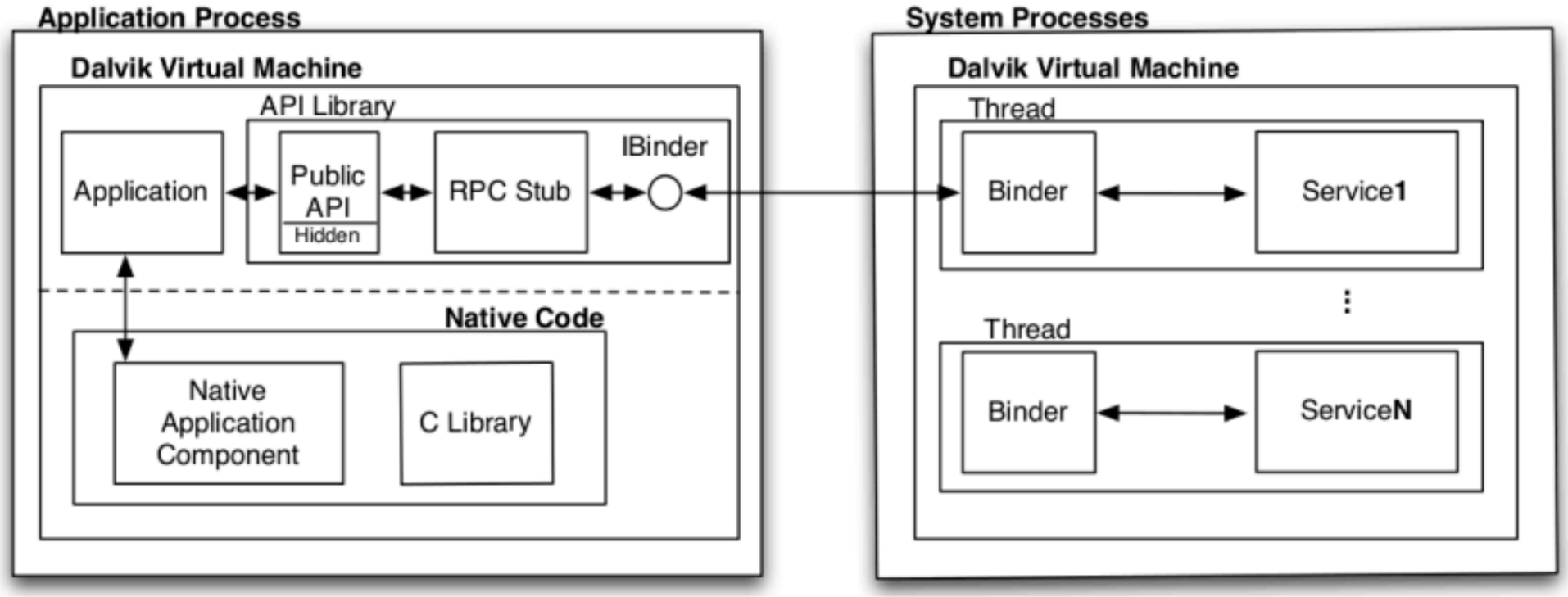
How Android Applications work (3)

- register-based architecture (JVM is stack-based)
  - Java VM cannot execute Dalvik code
  - 16-bit instructions
  - copy-on-write memory sharing
  - dx cross-compiler - works with javac output

Compiling applications



Android architecture



AndroidManifest

- XML configuration file, Every application must have it
- Contains:
  - application's name, icon, labels
  - linked libraries
  - application components: <activity>, <service>, <receiver>, <provider> tags
  - Activity shown at launch time
  - Intent filters
  - **Permissions**

AndroidManifest Example

Panoramio App:

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.google.android.panoramio">
    <application android:icon="@drawable/icon">
        <activity android:name=".Panoramio" android:label="@string/app_name"
                android:theme="@style/Theme.Panoramio">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

                <activity android:name=".ImageList" android:label="@string/app_name"
                        android:theme="@android:style/Theme.Light"/>

                <activity android:name=".ViewImage" android:label="@string/app_name"
                        android:theme="@style/Theme.Panoramio"/>

        <activity android:name=".ViewMap" android:label="@string/app_name"/>

                <uses-library android:name="com.google.android.maps" />
    </application>
        <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
        <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
</manifest>
```

Application Framework Security

- Android Framework Security → coarse-grained control
- Mandatory Access Control(MAC) enforced by middleware

Application Framework Security

- Components protected using access permission labels
  - declared in the AndroidManifest file
  - can not be changed after installation
  - 4 protection levels
    - normal - always granted
    - dangerous - requires user approval
    - signature - matching certificate
    - signature or system - matching certificate with system image

Permissions

- At install-time each application requests a list of permission
- All permissions must be granted at install time - all or nothing
- Protect access to Android components, services and APIs
  - e.g API for access to phone's hardware
  - ~130 API-defined permissions in Manifest. Permissions class

Permissions

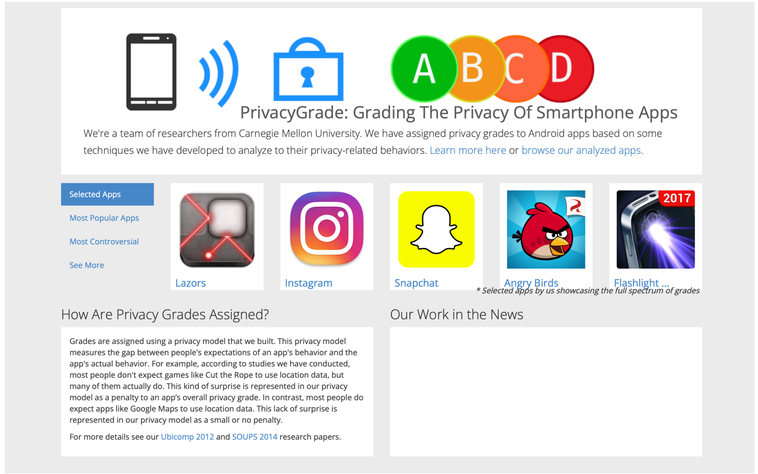
- No custom-defined permissions by developers
  - name conflicts may appear
  - current research on Android permissions doesn't take them into consideration
- PackageManagerService in the middleware checks the permissions for a request

User Attention, Comprehension, and Behavior

- Are users paying attention to the permissions?
- Do users understand the permissions?
- Can users make correct security decisions?
- Results: too few users comprehend or pay attention

Research around Android permissions

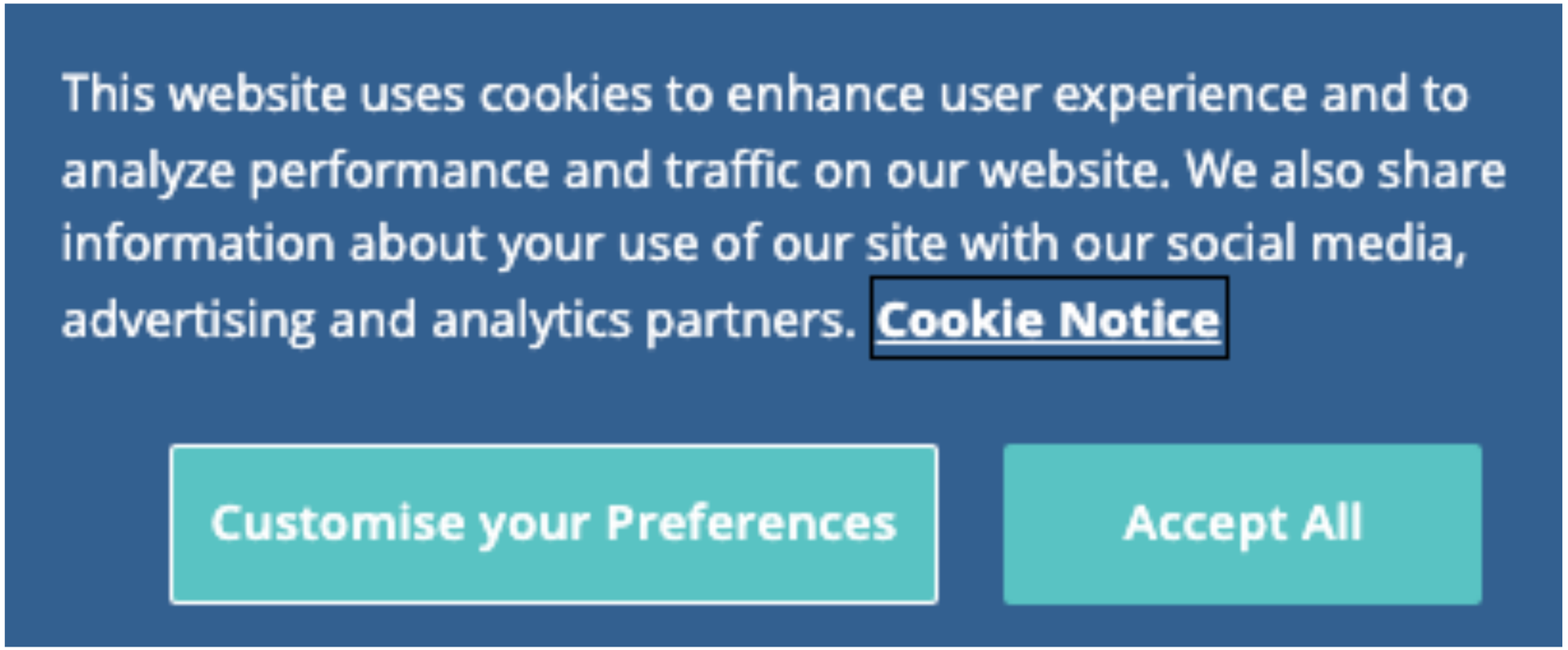
- The problem: unnecessary use of permissions
- The proposed solution: static analysis of API calls
- Permission map -
  - identifies permissions for Intents, Content Provides, API calls
  - determines if an app is overprivileged or not



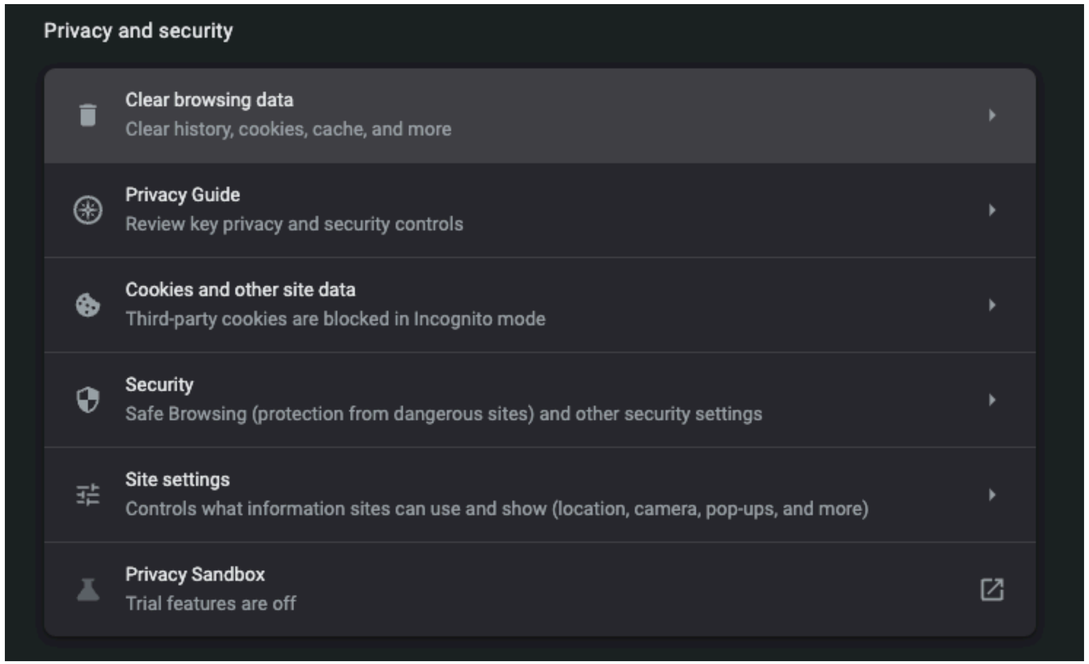
Research methods for Android Permissions

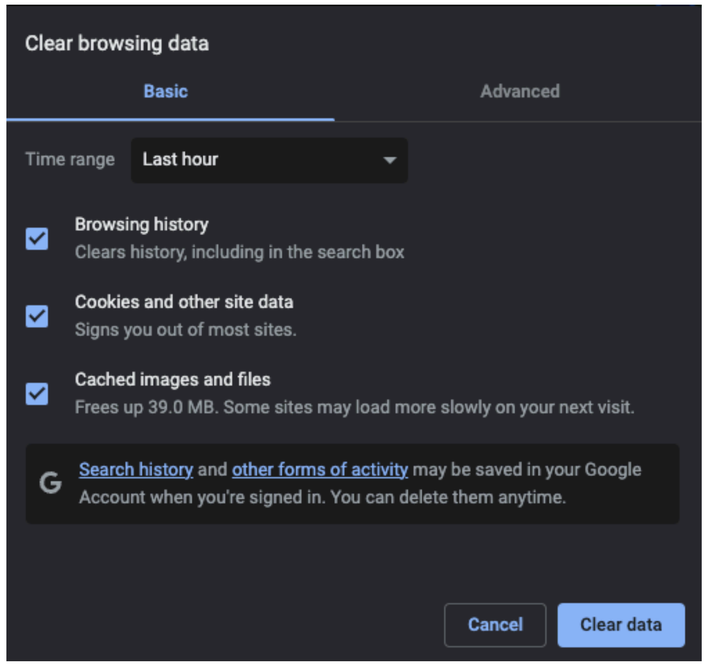
- Static analysis:
  - Map of permissions for each method in the Android API
- Dynamic analysis:
  - Log permission checks - modified middleware
- Blackbox test:
  - test cases for API calls, Intents, Content Providers

Cookie consent banner

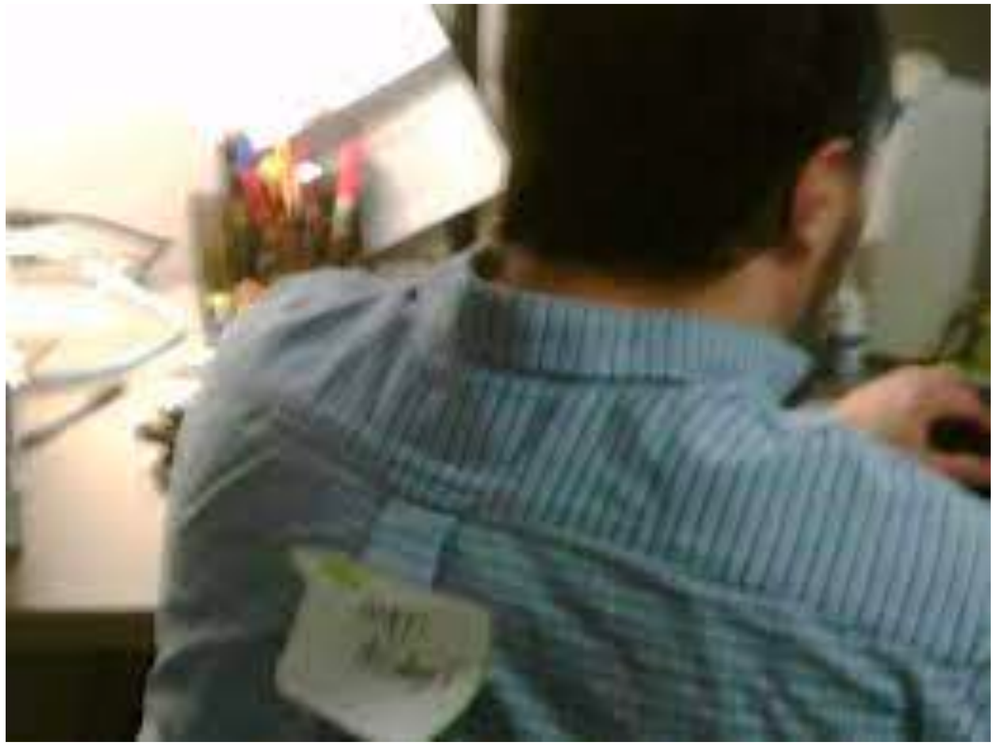


What is Cookie?



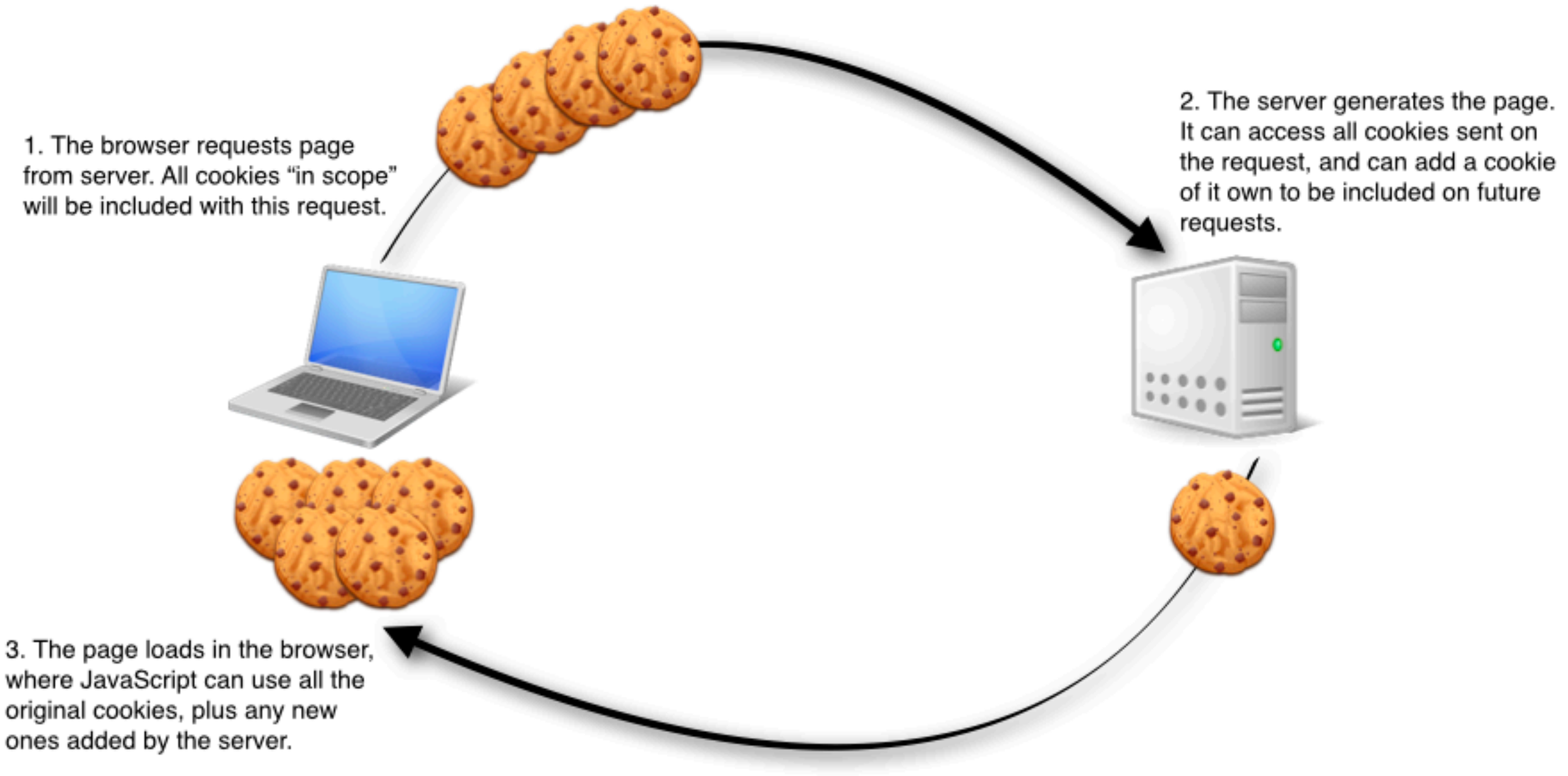


Cookie applications

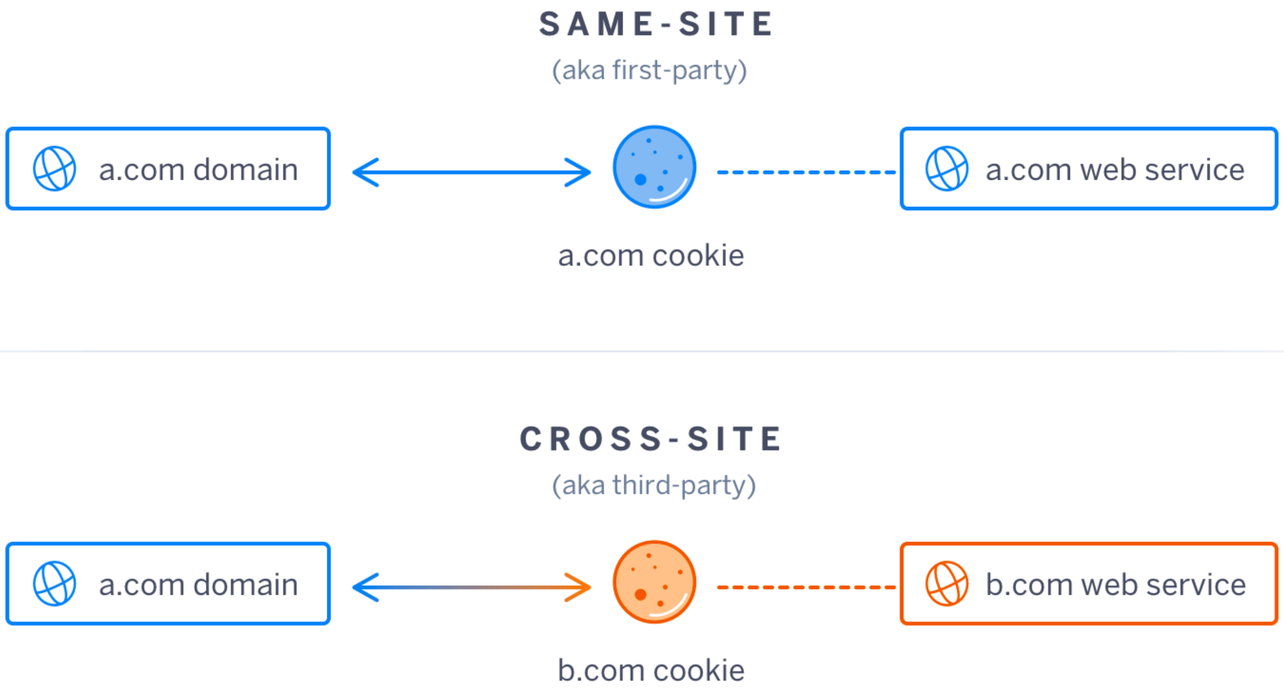


- Login status
- Signout personalization
- Anti-fraud
- Advertisement
- Marketing measurement
- …

Cookie: stateless to stateful



SameSite Cookie (Feb. 2020)



Starting February 4, 2020, Google Chrome will stop sending third-party cookies in cross-site requests unless the cookies are secured and flagged using an IETF standard called **SameSite**.

How Advertisements work?

1

User browses through a website : example.com

User behavior are sent to partner and a user id is assigned on a 3rd party cookie. (on google.com)

2

1. requests sent to google.com in order to have data associated to the user id

2. User ID assigned to a cookie on google.com domain (cookie ID)

3

User arrives on the publisher website (show-example.com) , where he is unknown

Required by Multiple Laws

Cookie Banner Guidelines for Each Global Privacy Regulation

In this article, we'll look at cookie banner best practices according to GDPR, CCPA, ICO, CNIL, LGPD, and the Nevada Privacy Law (SB-220) to help websites stay compliant.

Last Updated: August 5, 2022

01 GDPR Cookie Banner

The **General Data Protection Regulation** (GDPR) is the privacy regulation in force in the EU. The regulation went into effect on May 25, 2018, so many website owners are already familiar with GDPR cookie banner requirements.

One of the central protections GDPR gives EU citizens is that they have the right to be informed when businesses collect data about them. Businesses must let individuals know why they are collecting the data, how long they keep the data for, and which organizations they will share the data with. Individuals also have the right to object to the processing of their personal data in some

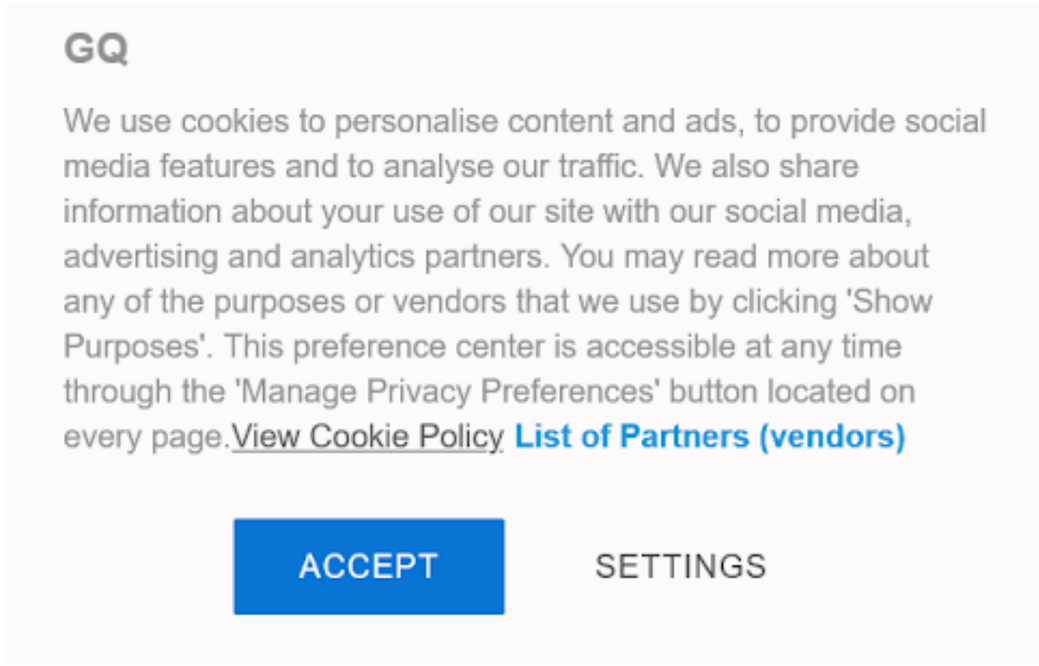
You Might Als

GDPR Con

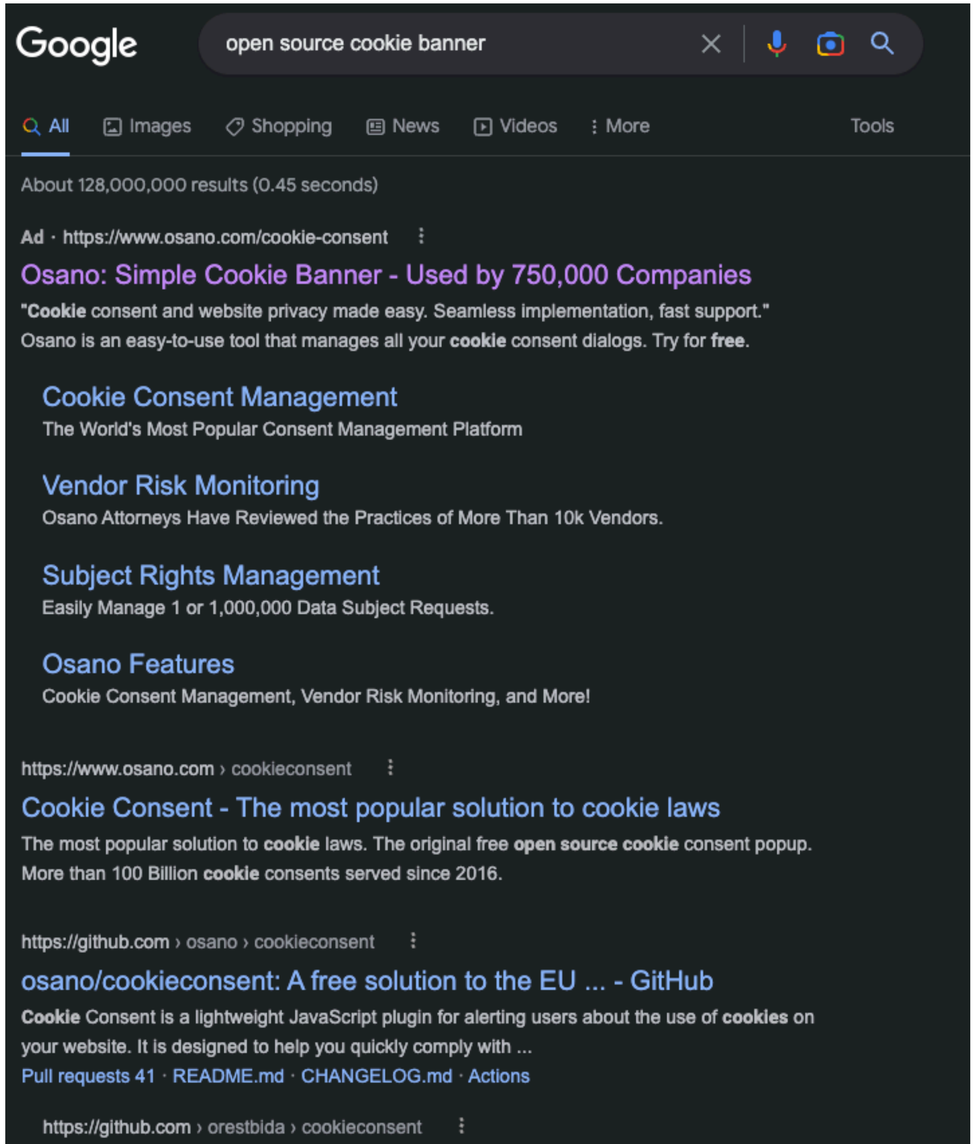
https://www.cookiepro.com/knowledge/cookie-banner-guidelines/

GDPR Banner requirements

- Include a Button to Accept Cookies
- Provide Detailed Information About Cookie use
- Alert the users if the website shares data with third parties
- Link to the website’s cookie policy
- Include a link to the cookie settings



How developers implement them?

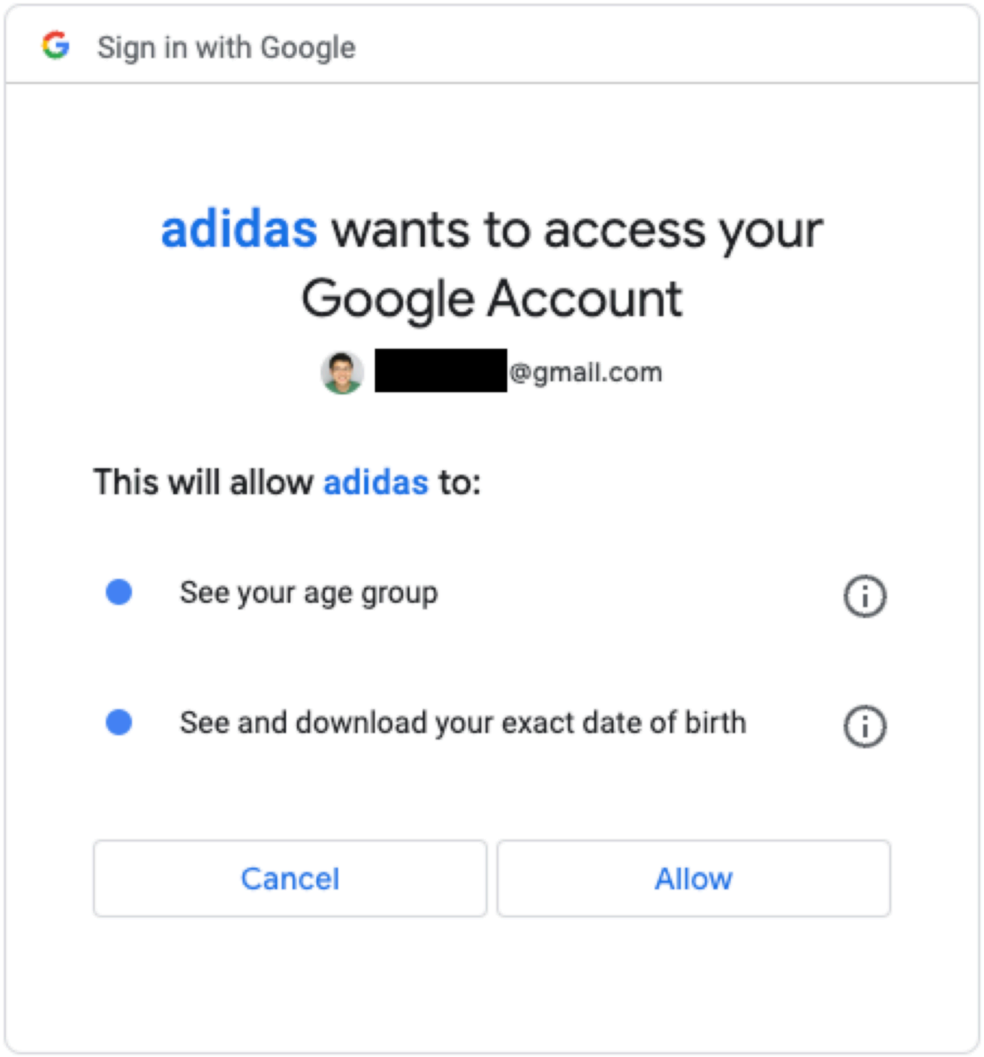


- Easy development
- One for all solutions
- Advertisements on high consent rates.

Issues

- Users do not care.
- Developers do not care.
- Advertisers are happy.
- Default opt-in.
- Decentralized management.
- No way to enforce.

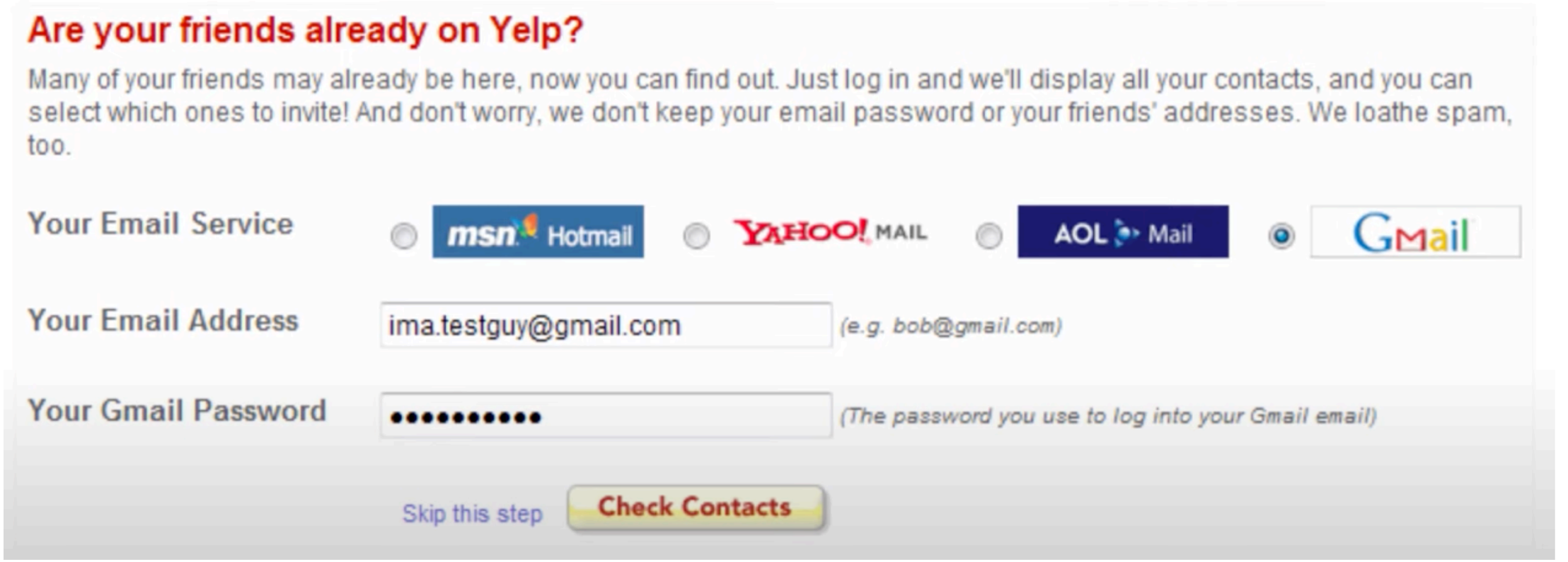
OAuth



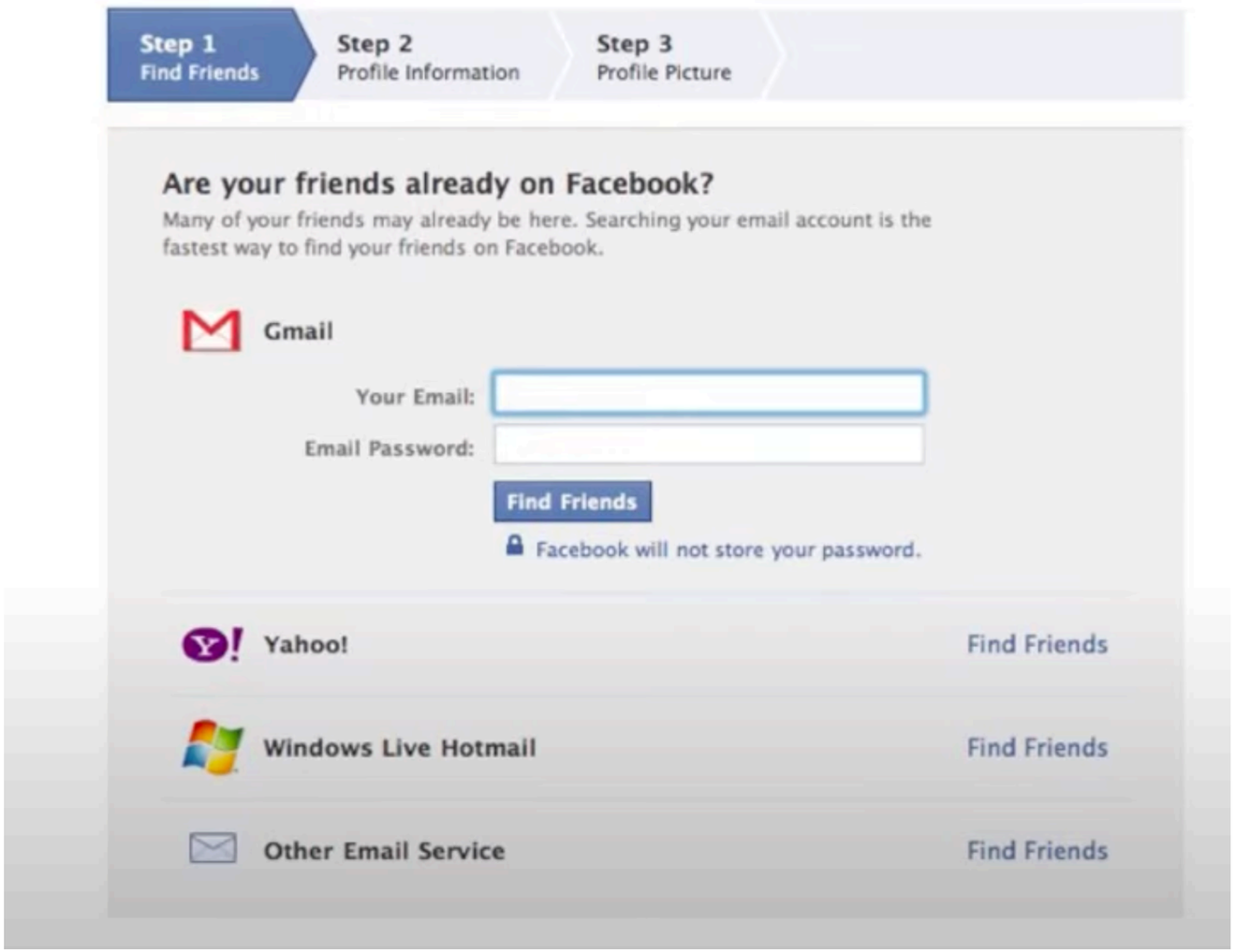
- How can I let a website access my data?
- Without giving it my password?

Identity use cases (since 2007)

- Simple login - forms and cookies
- Single sign-on across sites
- Mobile app login
- Delegated authorization

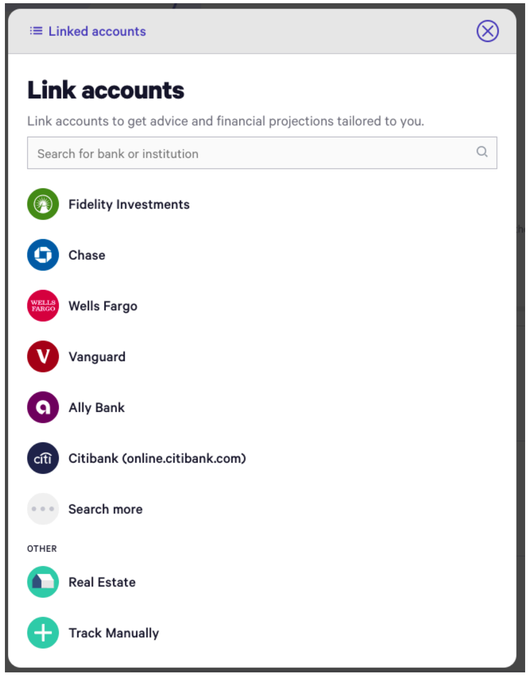


https://youtu.be/KT8ybowdyr0?t=50



https://youtu.be/KT8ybowdyr0?t=79

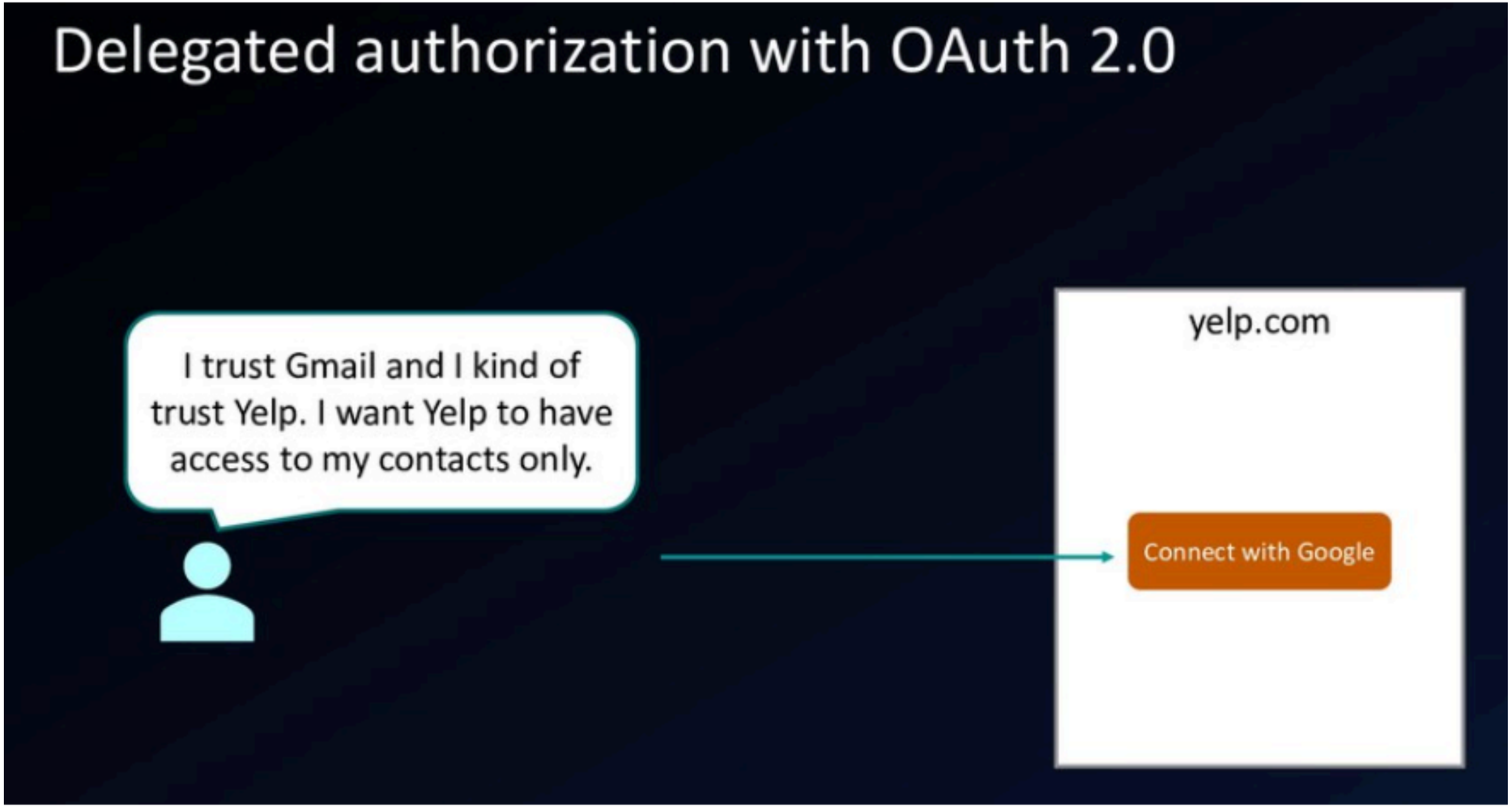
Today!

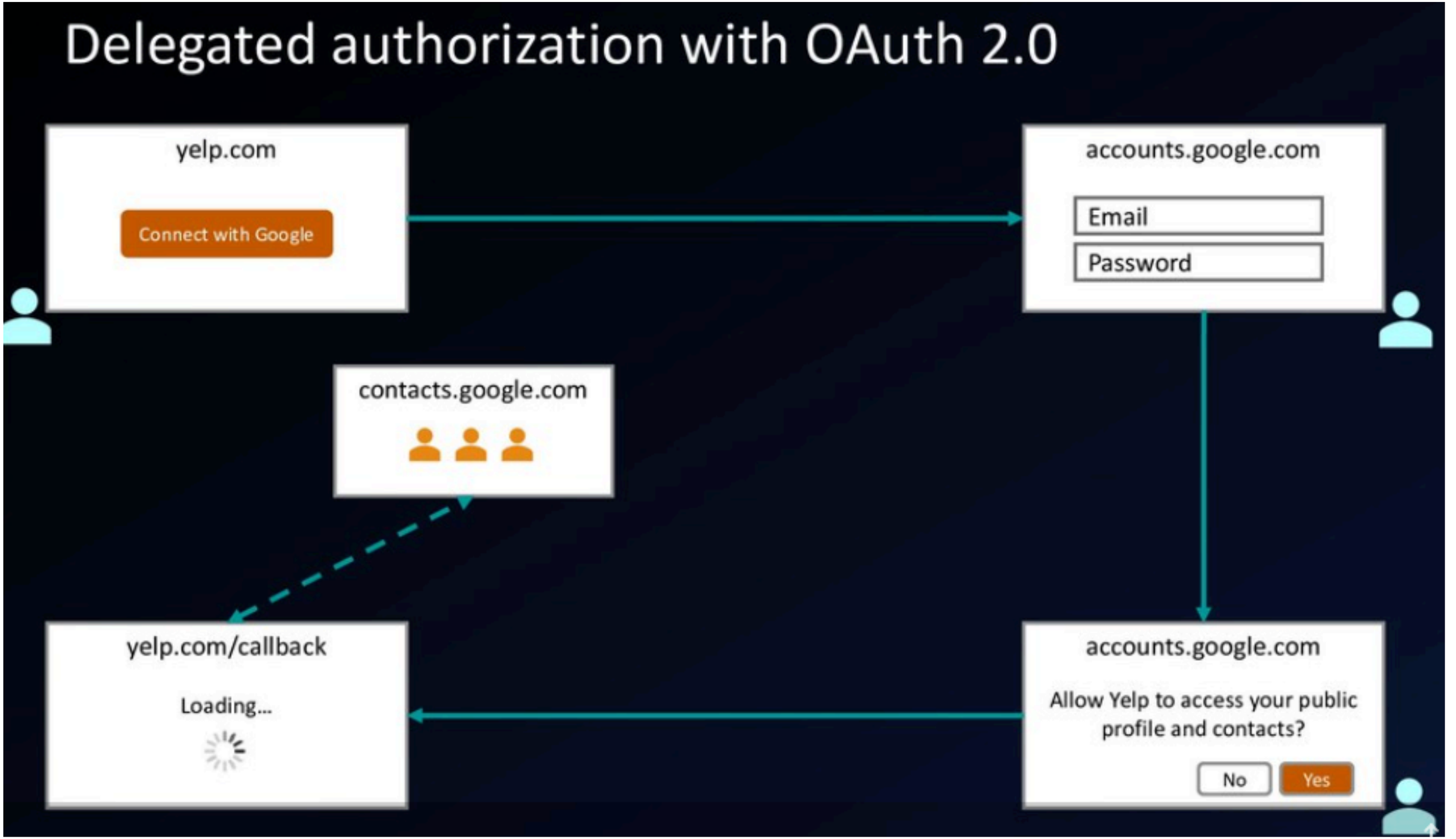


Once you select your institution, you'll be prompted to enter your username and password with that bank or brokerage, and we'll then link to your account. Your security is important to us. We use bank-level security to keep your account safe. Linking does not allow Wealthfront to manage or transfer assets in your linked account. Below are some related FAQs:

https://support.wealthfront.com/hc/en-us/articles/115000311663-How-do-I-link-an-outside-account-to-Wealthfront-

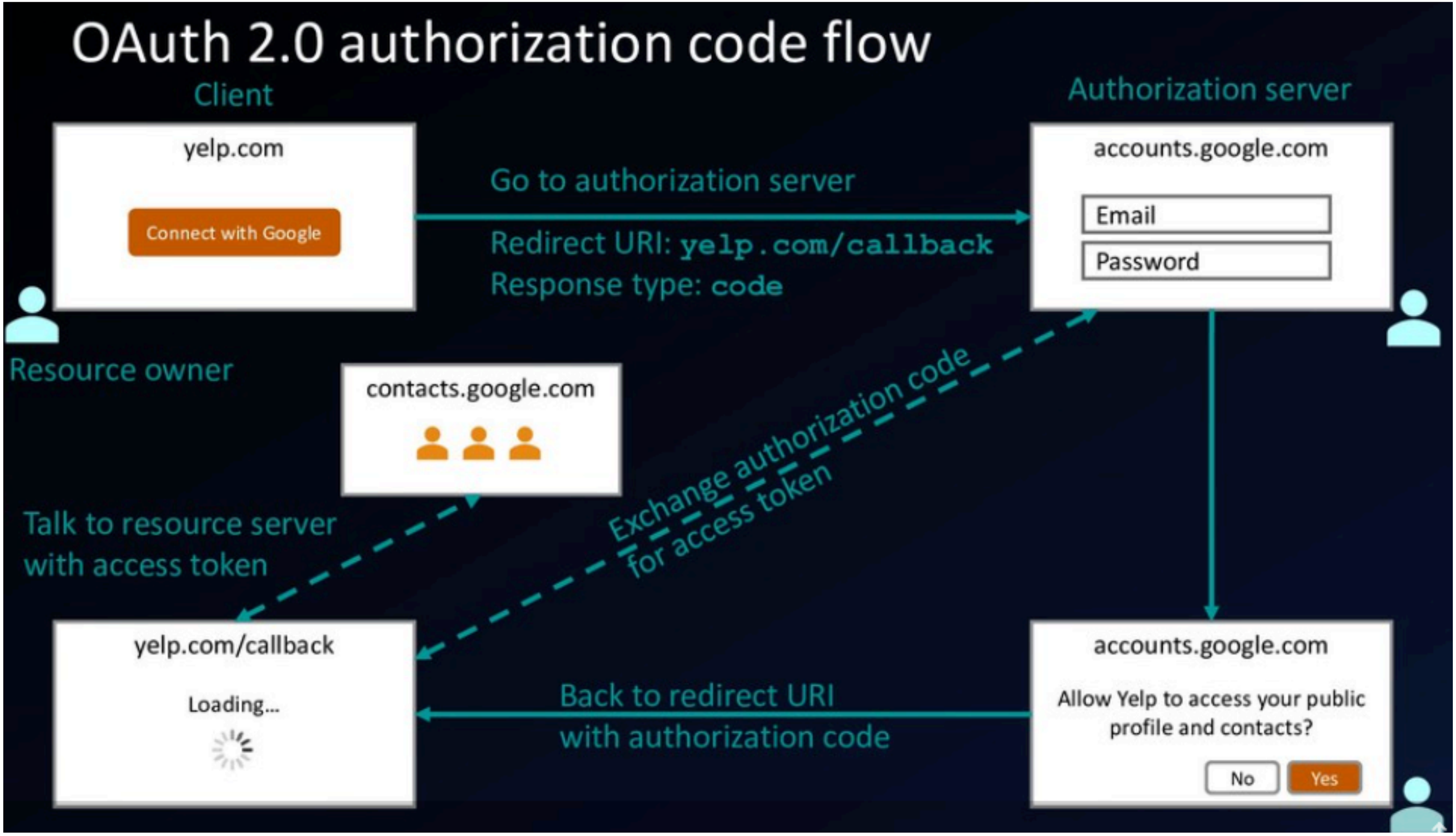
Problem formulation




Delegated authorization with OAuth 2.0
yelp.com
Connect with Google
accounts.google.com
Email
Password
contacts.google.com
yelp.com/callback
Loading...
accounts.google.com
Allow Yelp to access your public profile and contacts?
No
Yes

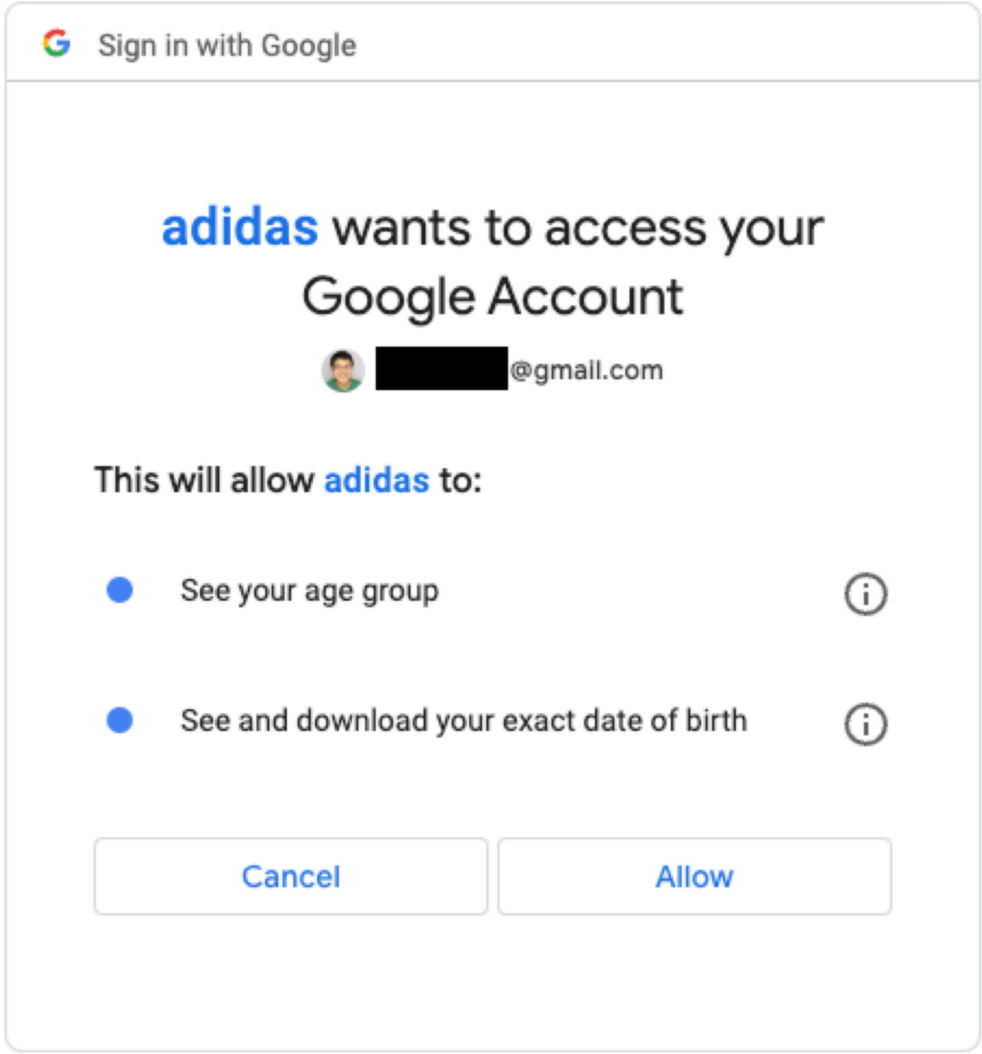
OAuth 2.0 Terminology

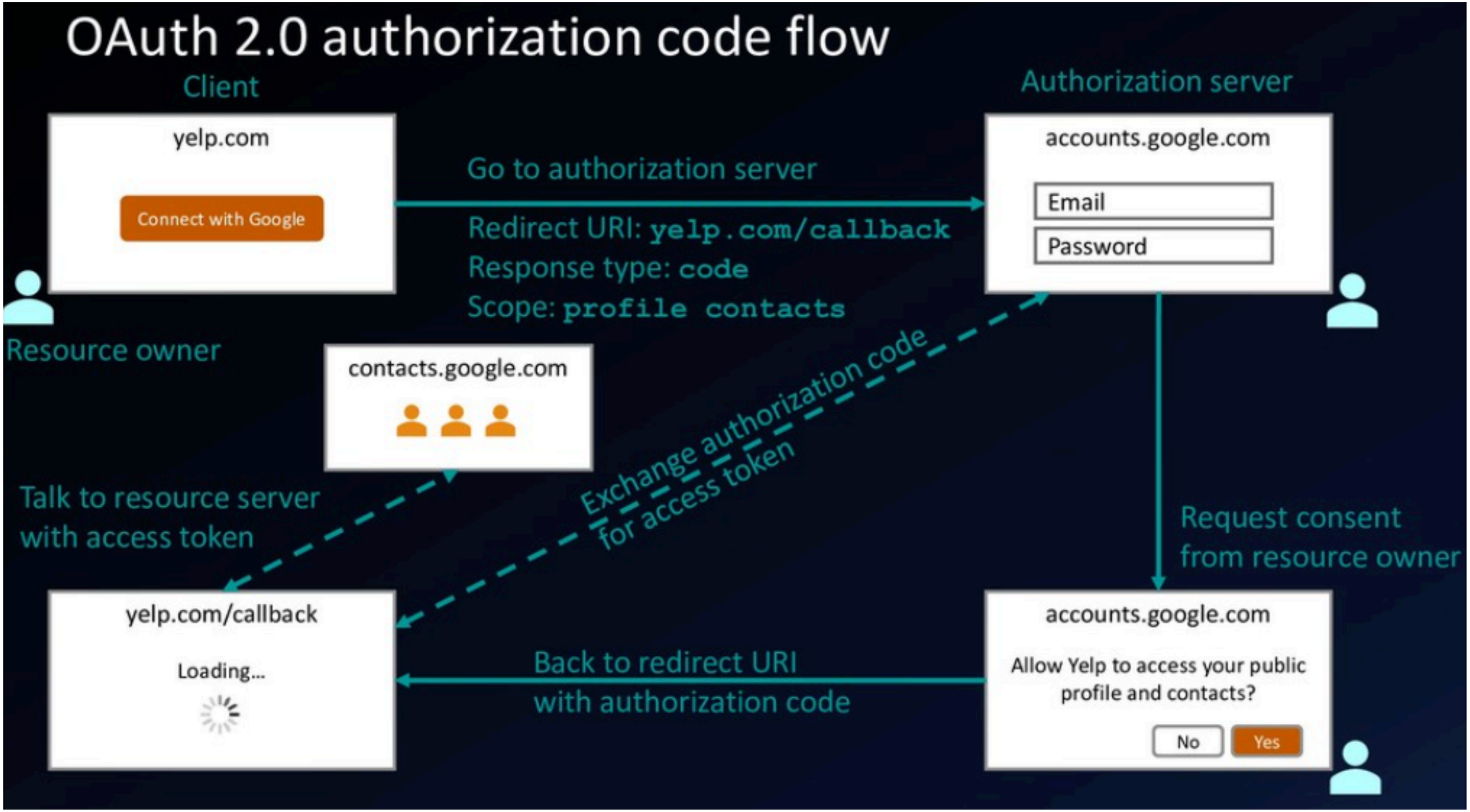
- Resource owner
- Client
- Authorization server
- Resource server
- Authorization grant
- Access token


OAuth 2.0 authorization code flow
Client
yelp.com
Connect with Google
Authorization server
accounts.google.com
Email
Password
Go to authorization server
Redirect URI: yelp.com/callback
Response type: code
Resource owner
contacts.google.com
Exchange authorization code for access token
Talk to resource server with access token
yelp.com/callback
Loading...
Back to redirect URI with authorization code
accounts.google.com
Allow Yelp to access your public profile and contacts?
No
Yes

More Terminology

- Scope
- Consent
- Front channel
- Back channel




OAuth 2.0 authorization code flow
Client
yelp.com
Connect with Google
Authorization server
accounts.google.com
Email
Password
Go to authorization server
Redirect URI: yelp.com/callback
Response type: code
Scope: profile contacts
Resource owner
contacts.google.com
Exchange authorization code for access token
Talk to resource server with access token
Request consent from resource owner
yelp.com/callback
Loading...
Back to redirect URI with authorization code
accounts.google.com
Allow Yelp to access your public profile and contacts?
No
Yes

Starting the flow

```
https://accounts.google.com/o/oauth2/v2/auth?
 client_id=abc123&
 redirect_uri=https://yelp.com/callback&
 scope=profile&
 response_type=code&
 state=foobar
```

Calling back

```
https://yelp.com/callback?
 error=access_denied&
 error_description=The user did not consent.
```

```
https://yelp.com/callback?
 code=oMsCeLvIaQm6bTrgtp7&
 state=foobar
```

Exchange code for an access token

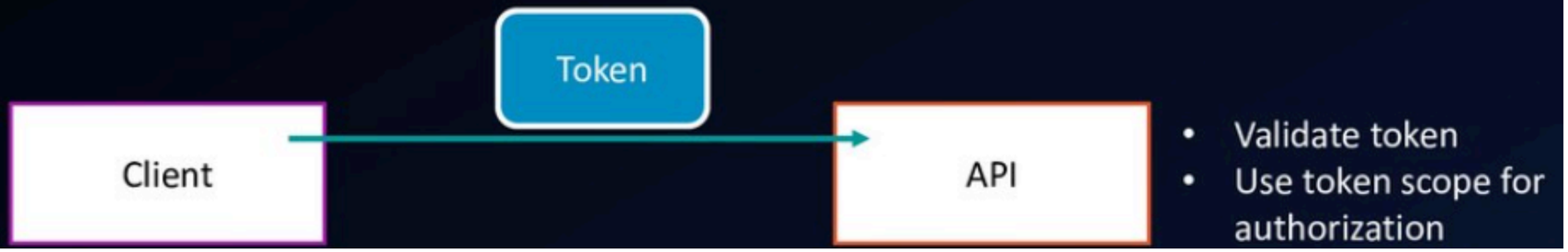
```
POST www.googleapis.com/oauth2/v4/token
Content-Type: application/x-www-form-urlencoded

code=oMsCeLvIaQm6bTrgtp7&
client_id=abc123&
client_secret=secret123&
grant_type=authorization_code
```

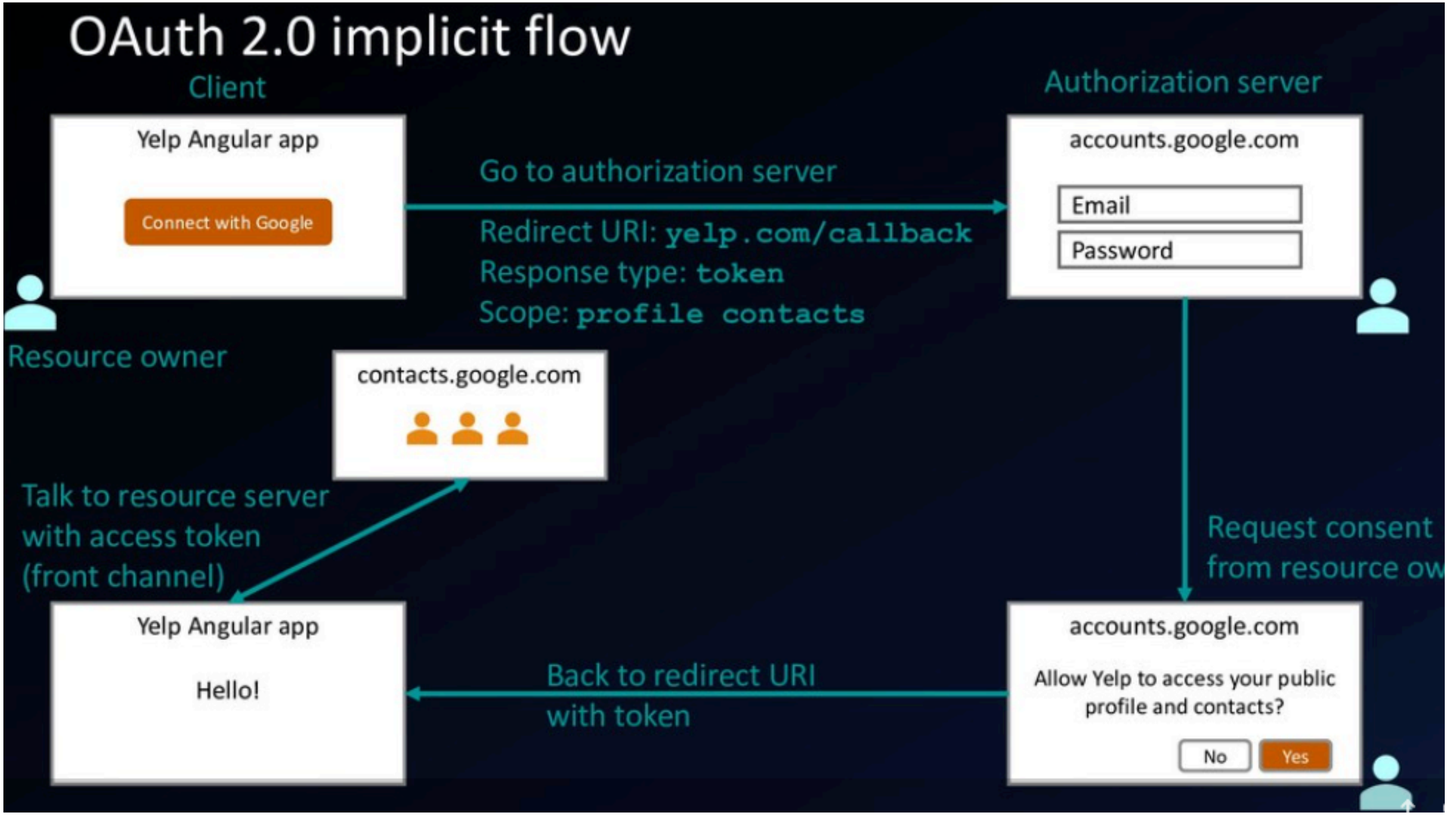
Authorization server returns an access token

```
{
  "access_token": "fFAGRNJru1FTz70BzhT3Zg",
  "expires_in": 3920,
  "token_type": "Bearer",
}
```

Use the access token

```
GET api.google.com/some/endpoint
Authorization: Bearer fFAGRNJru1FTz70BzhT3Zg
```



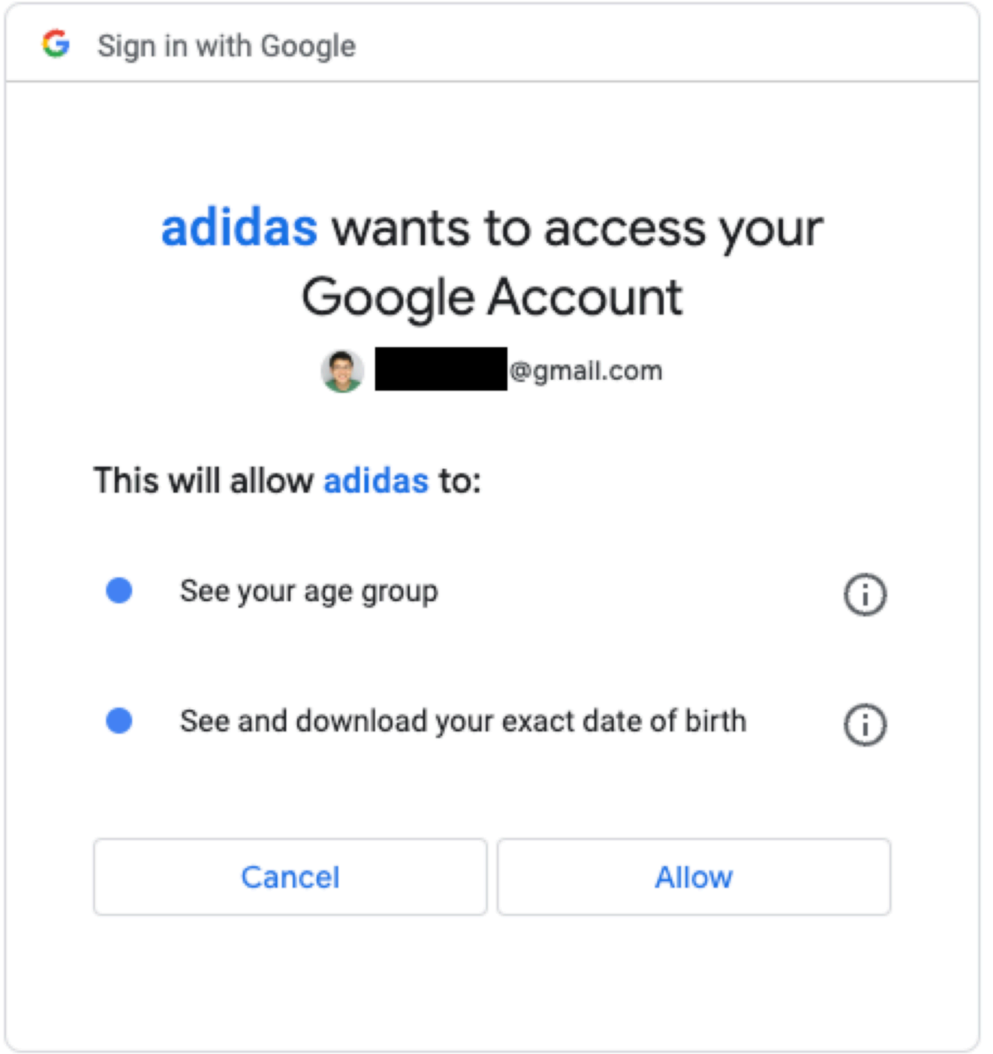

OAuth 2.0 implicit flow
Client
Yelp Angular app
Connect with Google
Authorization server
accounts.google.com
Email
Password
Go to authorization server
Redirect URI: yelp.com/callback
Response type: token
Scope: profile contacts
Resource owner
contacts.google.com
Talk to resource server
with access token
(front channel)
Request consent
from resource ow
Yelp Angular app
Hello!
accounts.google.com
Allow Yelp to access your public
profile and contacts?
No
Yes
Back to redirect URI
with token

Identity use cases (since 2007)

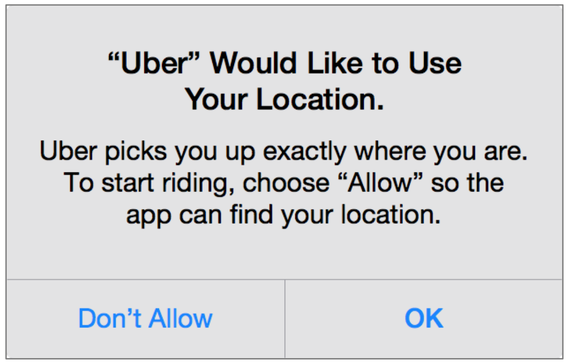
- Simple login - forms and cookies - Authentication
- Single sign-on across sites - Authentication
- Mobile app login - Authentication
- Delegated authorization - Authorization

Problems with OAuth

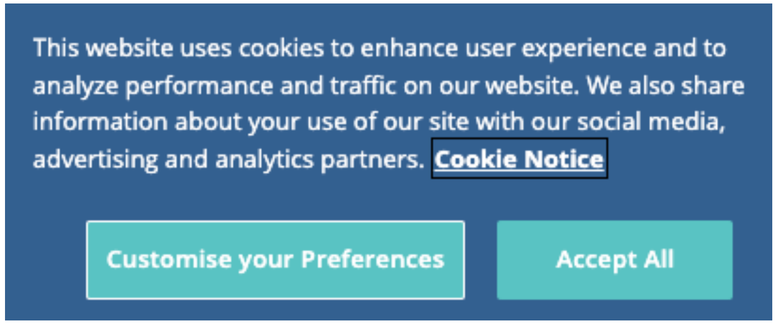
- No standard way to get the user's information
- Every implementation is a little different
- No common set of scopes
- Coarse granularity
- Users do not pay attention
- Hard to understand the terms



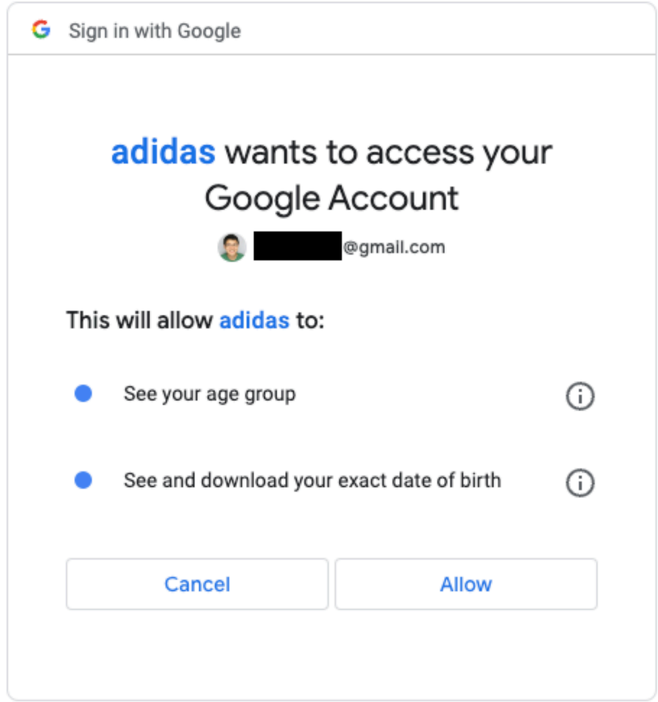
Recap: Three systems



Android permission

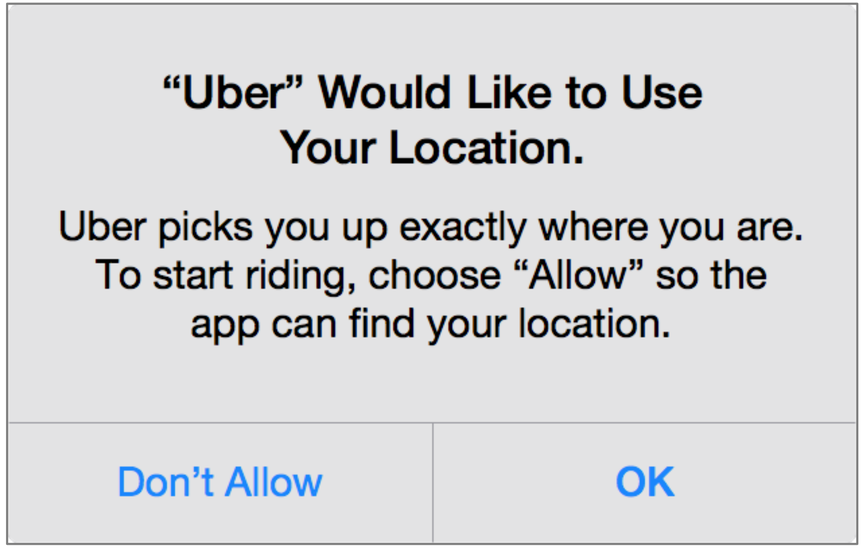


Browser cookie consent



OAuth

Recap: Key privacy concepts



- Control
- Notice
- Consent
- Usability
- System mechanisms