

User Privacy in OAuth-based Login, and a Standardized UI

OAuth Security Workshop, Nov 30, 2021

Srivathsan Morkonda Gnanasekaran, Sonia Chiasson, Paul C. van Oorschot

Ottawa, Canada

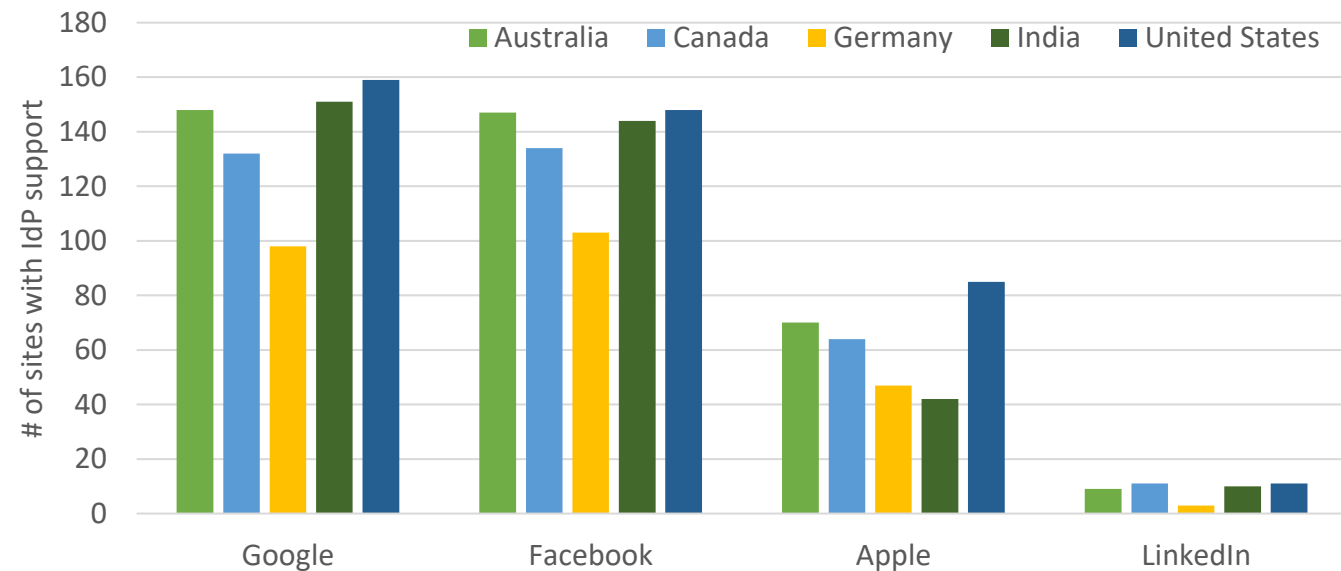


Carleton Security Research Labs
(CCSL+CISL)

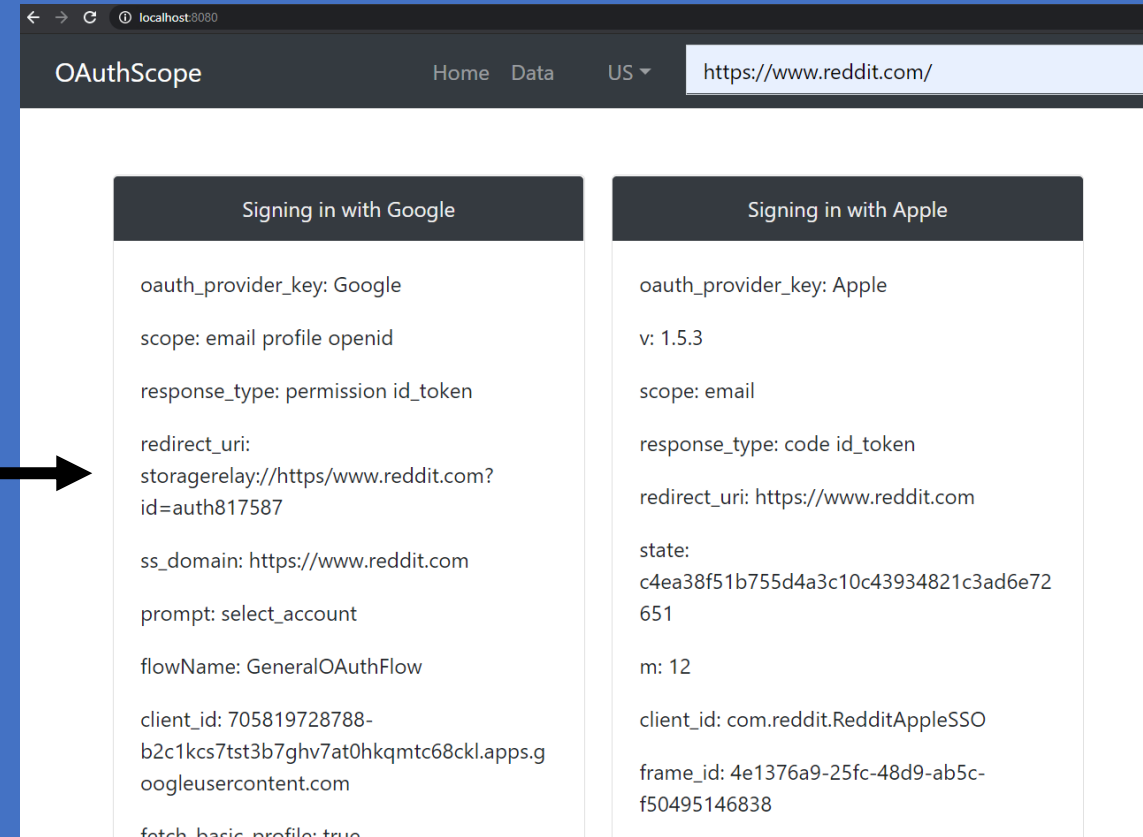
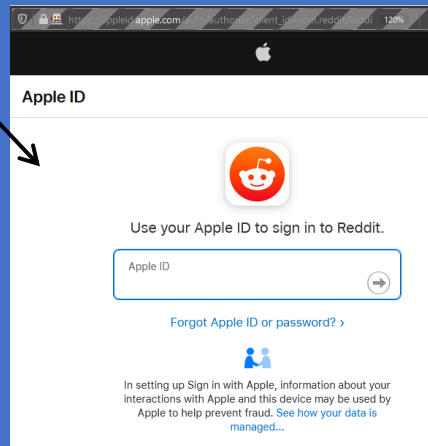
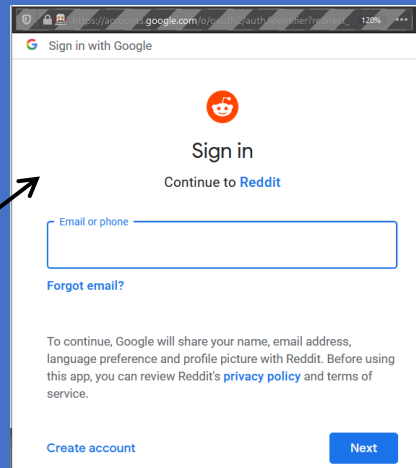
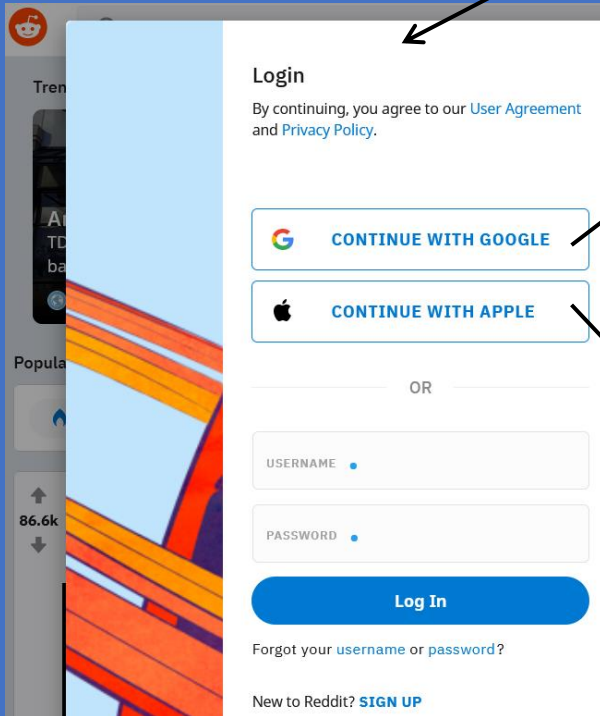
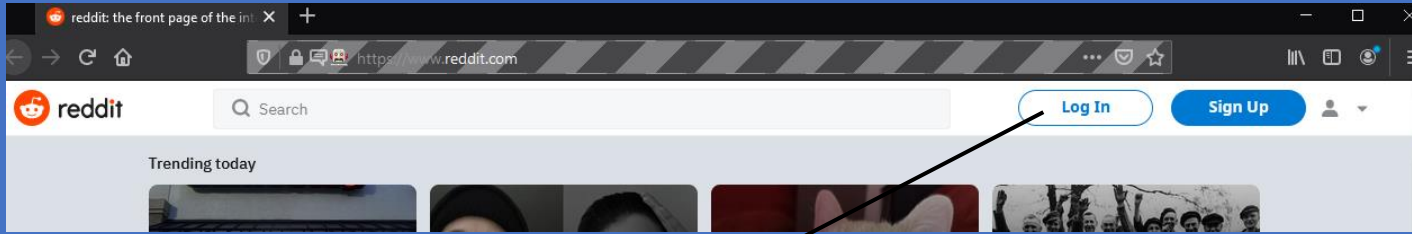


Our study

- We selected four ID Providers: Google, Facebook, Apple and LinkedIn
- Alexa Top 500 sites of each of five countries: AU, CA, DE, IN, US
- Using custom-built tool, we extracted OAuth 2.0 and OpenID Connect authorization requests made by RPs



Our Selenium-based OAuthScope tool

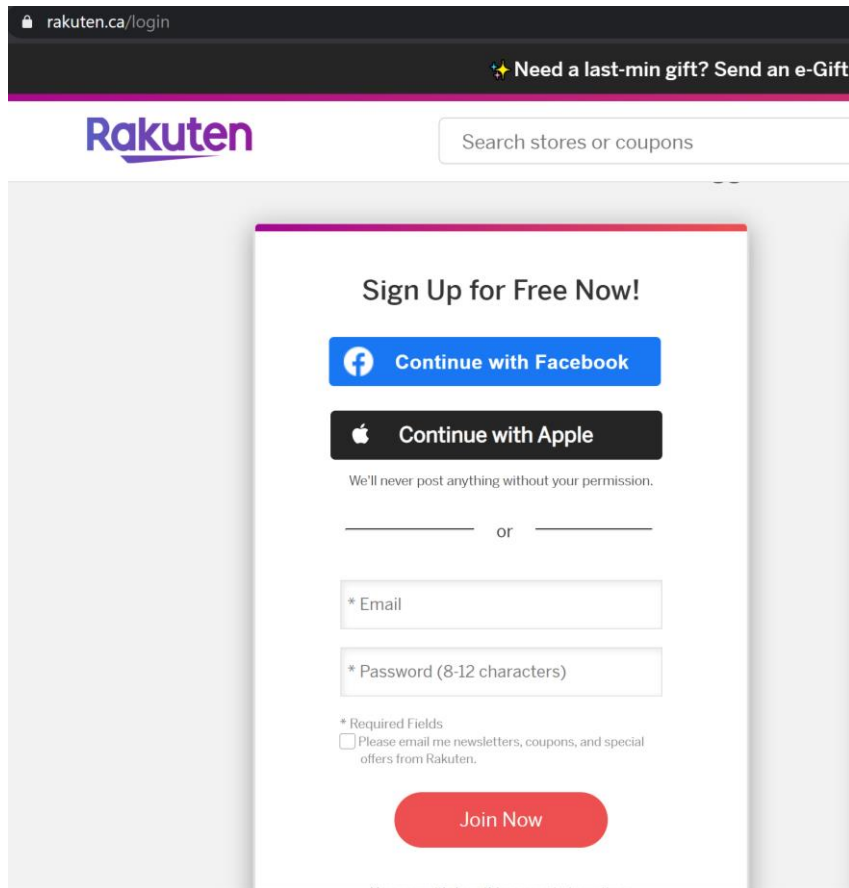


Our dataset

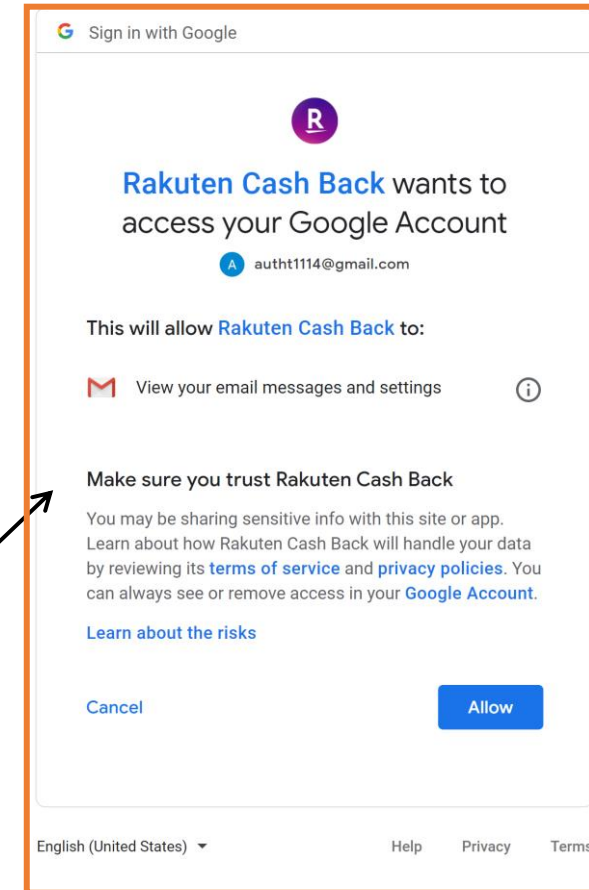
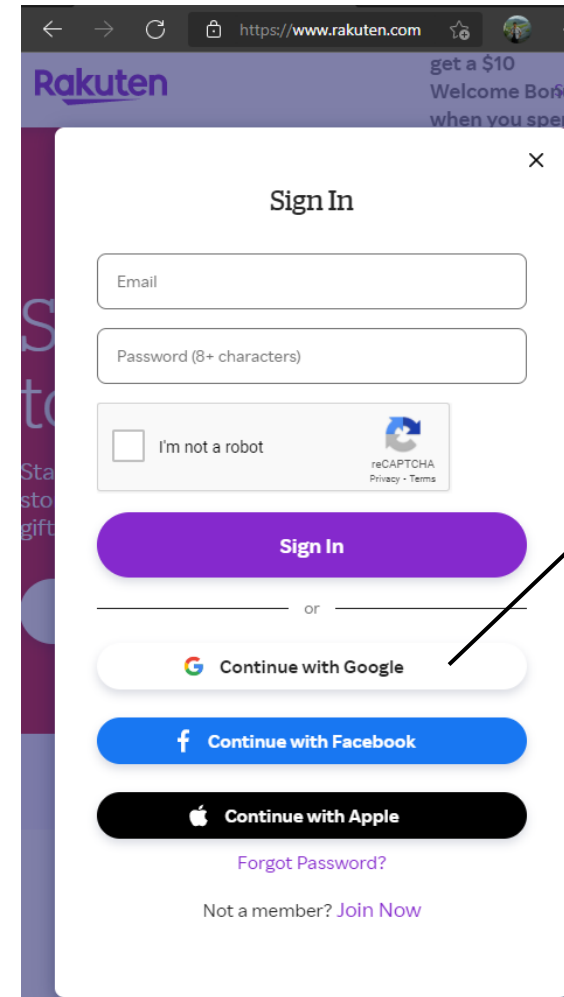
- Covers four ID providers (Google, Facebook, Apple, and LinkedIn) in top 500 sites in each of 5 countries
 - 2500 site visits in total
- We used VPNs when collecting data in a specific country
- We found 815 RPs with at least one of the 4 IdPs listed
 - Australia: 174
 - Canada: 159
 - Germany: 126
 - India: 172
 - United States: 184

Do RPs offer similar IdP options to users in different countries?

Rakuten.ca vs. Rakuten.com

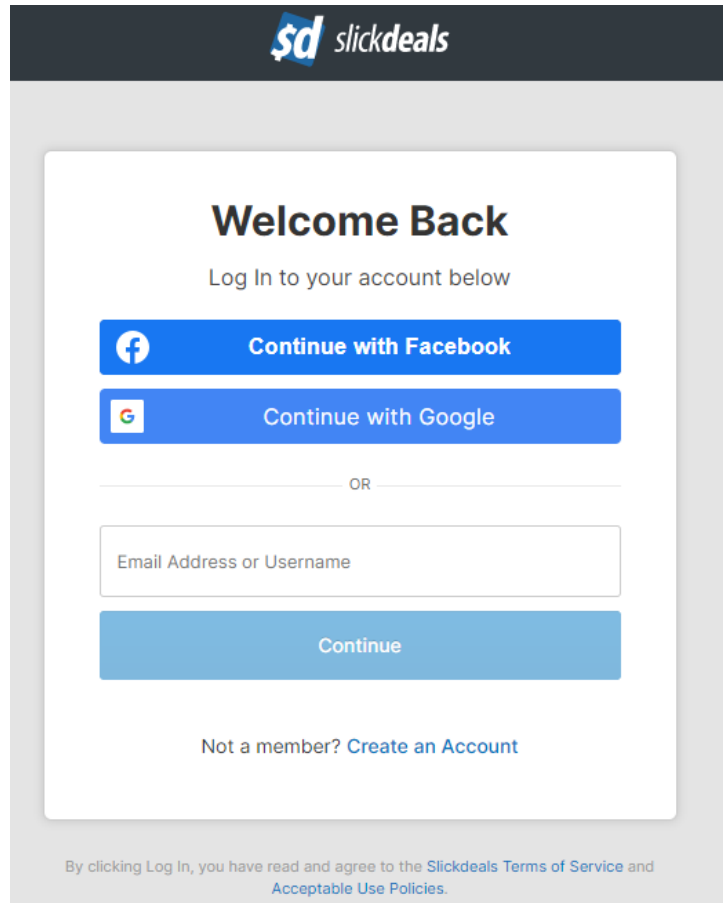


Rakuten.ca (Canada)

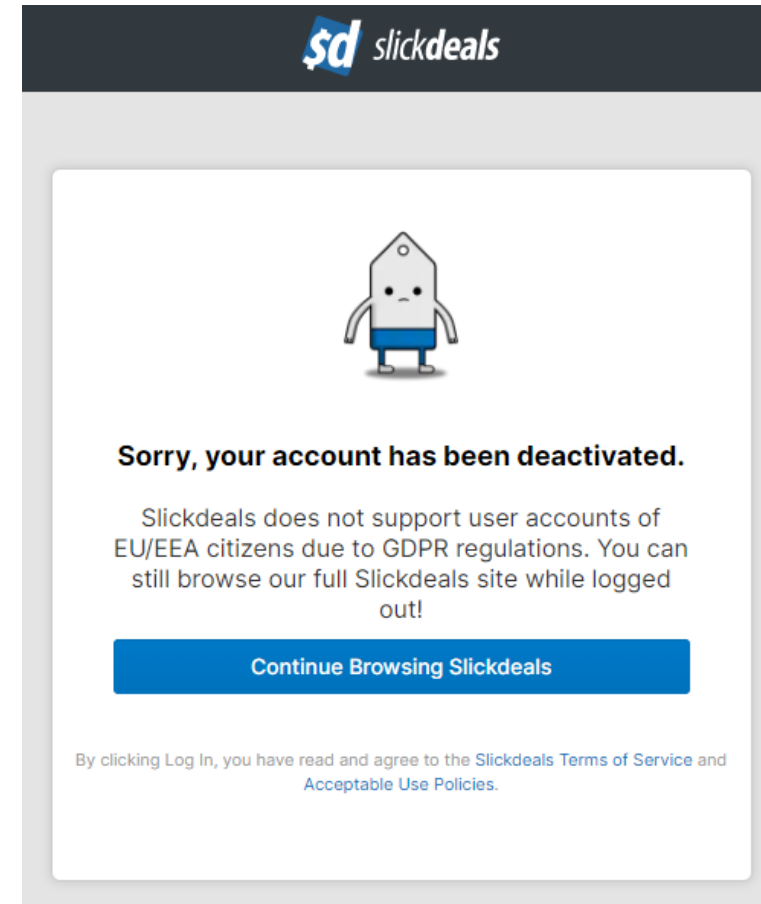


Rakuten.com (US)

Slickdeals.net in US and Germany

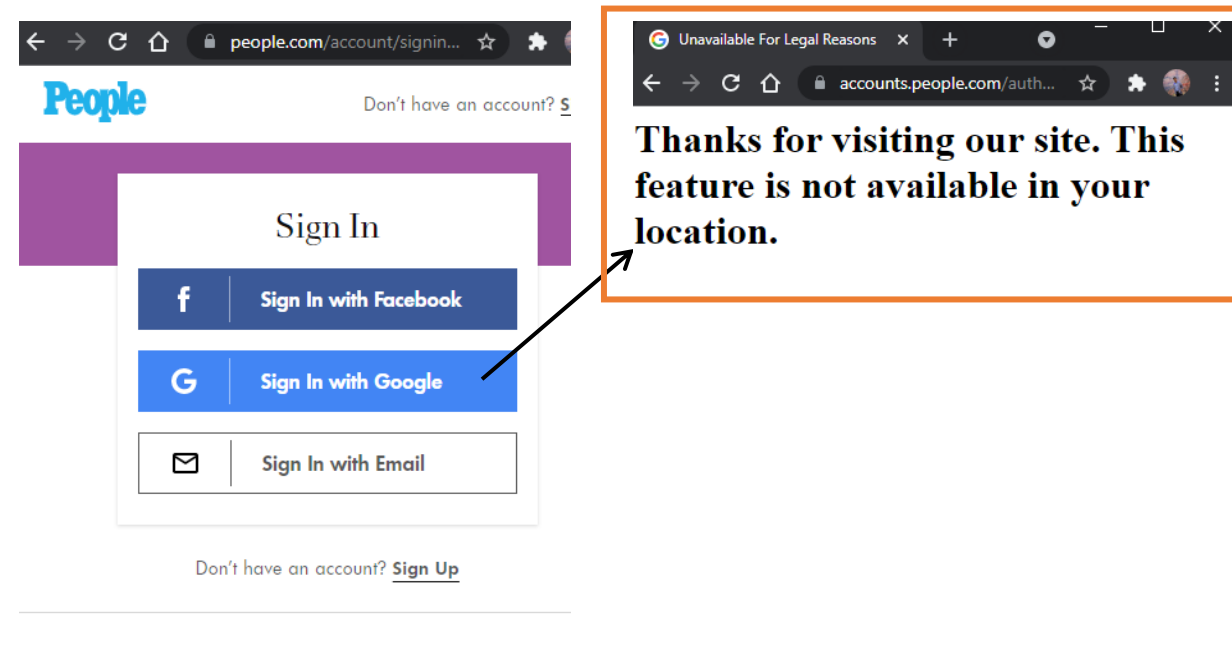
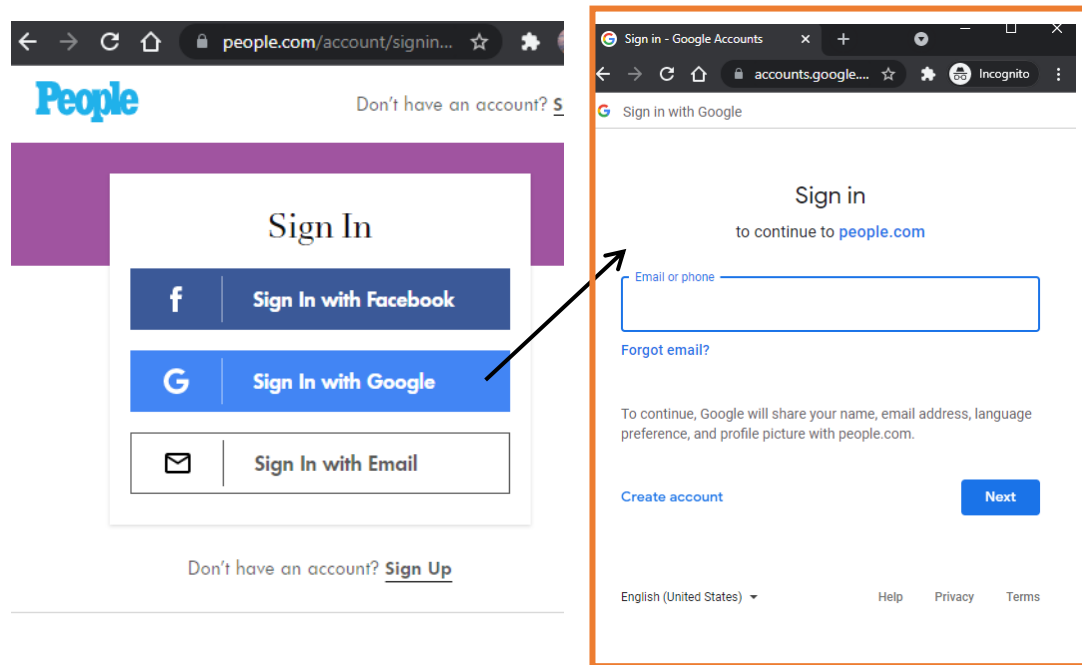


Site in US



Site in Germany

People.com in US and Germany



© Copyright 2021 Meredith Corporation. People is a registered trademark of Meredith Corporation. All Rights Reserved. People may receive compensation for some links to products and services on this website. Offers may be subject to change without notice. | Privacy Policy | Terms of Service | Ad Choice | Manage Push Notifications | California Do Not Sell | Web Accessibility

© Copyright 2021 Meredith Corporation. People is a registered trademark of Meredith Corporation. All Rights Reserved. People may receive compensation for some links to products and services on this website. Offers may be subject to change without notice. | Privacy Policy | Terms of Service | Ad Choice | Manage Push Notifications | California Do Not Sell | Web Accessibility

Site in US

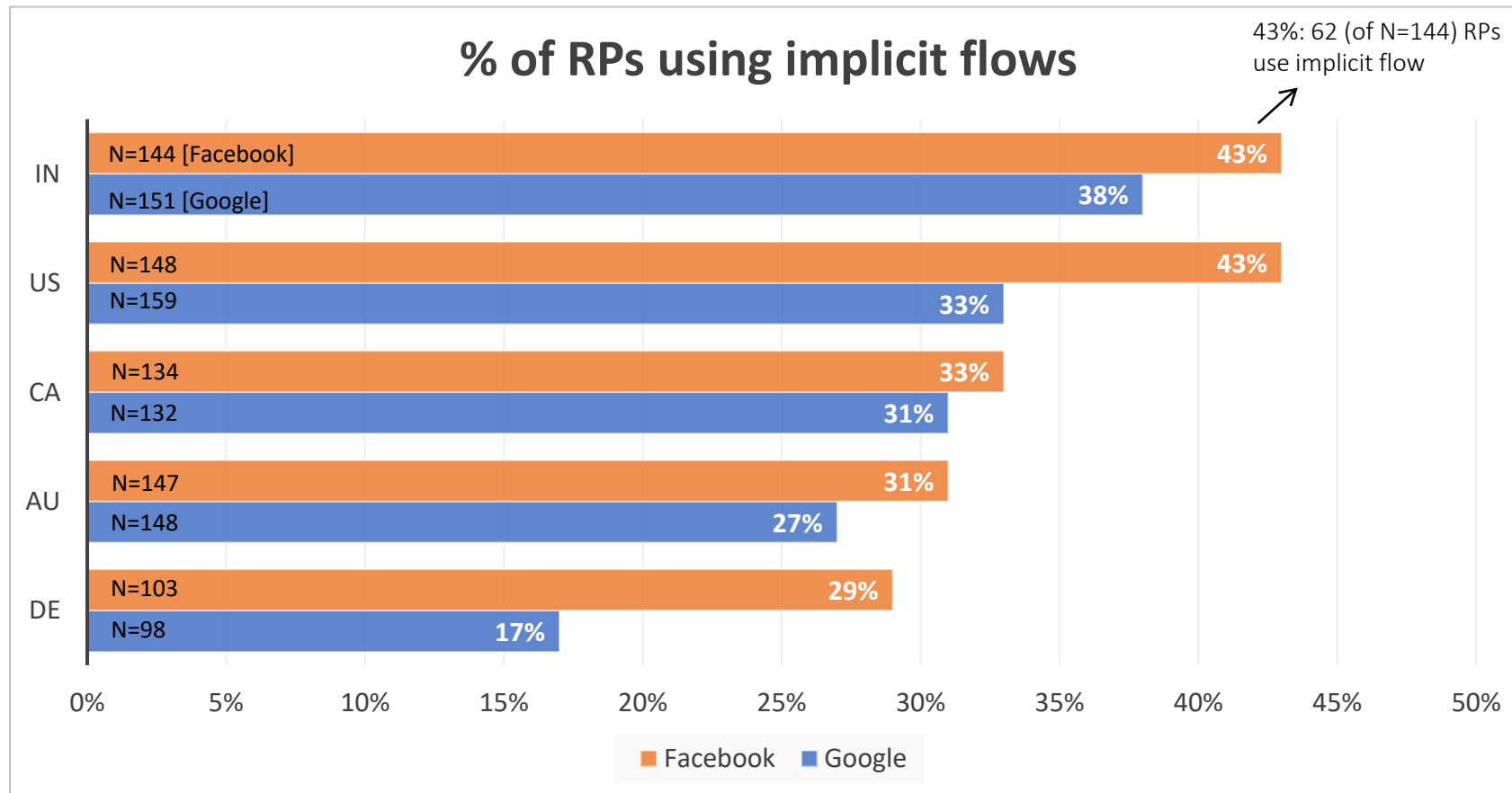
Site in Germany

RPs in US and Germany

- 80 of the 184 US RPs show a different site version in Germany
 - 17 of 80 offer fewer IdP choices
 - unable to collect data on 4 sites
 - No instances where sites in Germany requested more data than their US version
- Sites either state limitations due to GDPR or simply don't load the login page
- Fewer IdP choices for German users
 - Possibly a broader pattern for EU users

How many sites use the implicit flow?

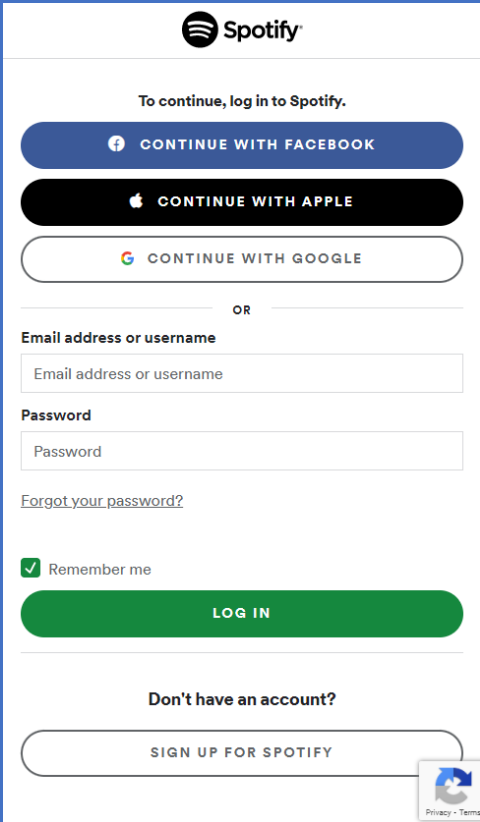
Use of Implicit flows



N: # of top 500 sites offering login option with the IdP

If a site supports multiple IdP logins,
how do they vary in privacy?

Different choices in Login dialog and Sign-Up dialog



Spotify

To continue, log in to Spotify.

CONTINUE WITH FACEBOOK

CONTINUE WITH APPLE

CONTINUE WITH GOOGLE

OR

Email address or username

Password

Forgot your password?

Remember me

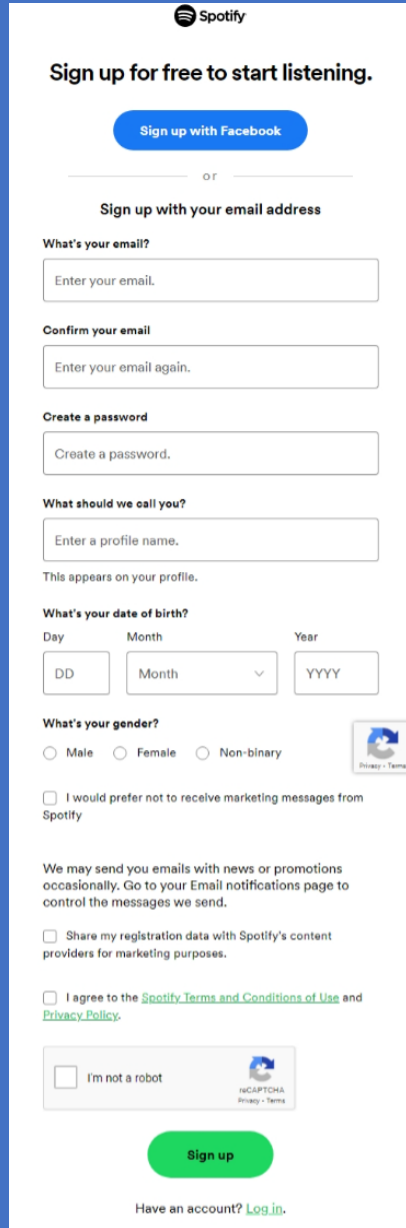
LOG IN

Don't have an account?

SIGN UP FOR SPOTIFY

[Privacy - Terms](#)

Spotify.com



Spotify

Sign up for free to start listening.

Sign up with Facebook

or

Sign up with your email address

What's your email?

Enter your email.

Confirm your email

Enter your email again.

Create a password

Create a password.

What should we call you?

Enter a profile name.

This appears on your profile.

What's your date of birth?

Day: DD, Month: Month, Year: YYYY

What's your gender?

Male Female Non-binary

I would prefer not to receive marketing messages from Spotify

We may send you emails with news or promotions occasionally. Go to your Email notifications page to control the messages we send.

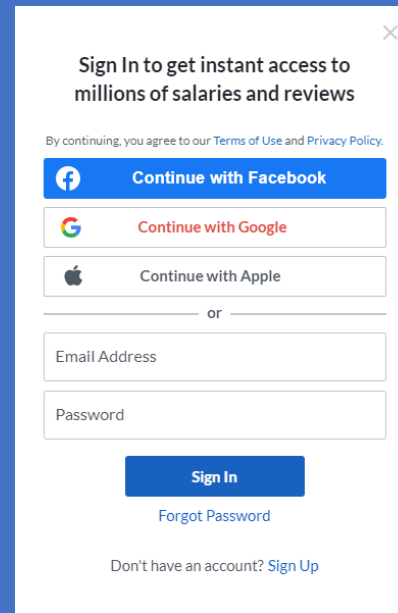
Share my registration data with Spotify's content providers for marketing purposes.

I agree to the [Spotify Terms and Conditions of Use](#) and [Privacy Policy](#).

I'm not a robot **reCAPTCHA**

Sign up

Have an account? [Log in](#).



Sign In to get instant access to millions of salaries and reviews

By continuing, you agree to our [Terms of Use](#) and [Privacy Policy](#).

Continue with Facebook

Continue with Google

Continue with Apple

or

Email Address

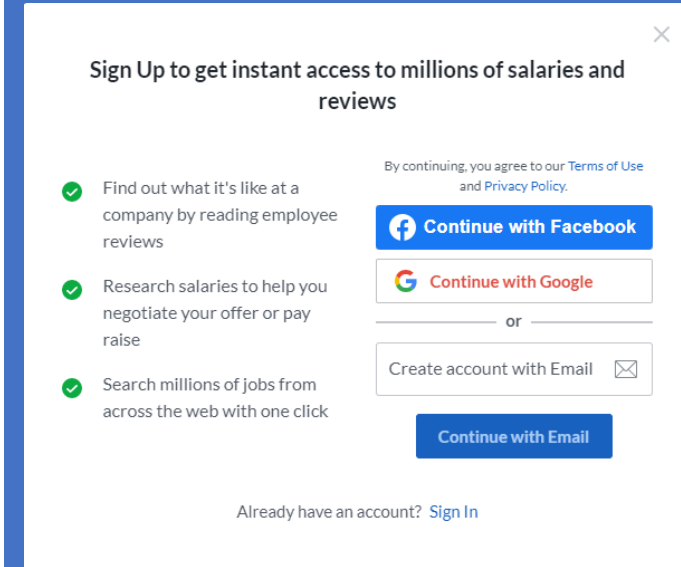
Password

Sign In

[Forgot Password](#)

Don't have an account? [Sign Up](#)

Glassdoor.ca



Sign Up to get instant access to millions of salaries and reviews

By continuing, you agree to our [Terms of Use](#) and [Privacy Policy](#).

- Find out what it's like at a company by reading employee reviews
- Research salaries to help you negotiate your offer or pay raise
- Search millions of jobs from across the web with one click

Continue with Facebook

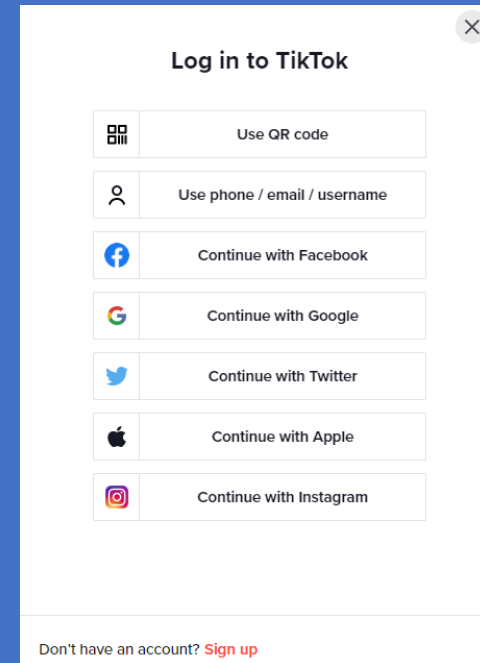
Continue with Google

or

Create account with Email

Continue with Email

Already have an account? [Sign In](#)



Log in to TikTok

Use QR code

Use phone / email / username

Continue with Facebook

Continue with Google

Continue with Twitter

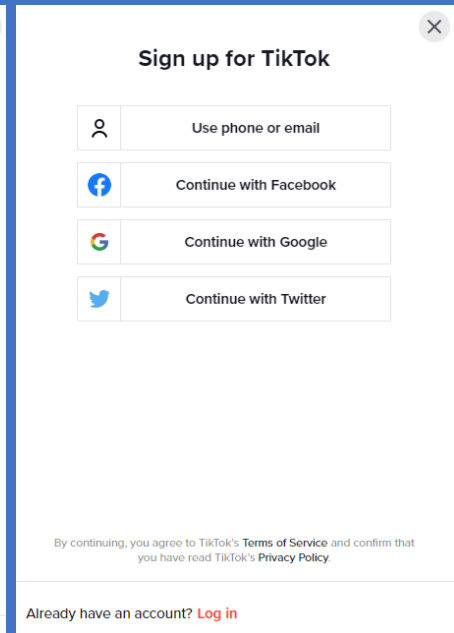
Continue with Apple

Continue with Instagram

By continuing, you agree to TikTok's [Terms of Service](#) and confirm that you have read TikTok's [Privacy Policy](#).

Already have an account? [Log in](#)

Don't have an account? [Sign up](#)



Sign up for TikTok

Use phone or email

Continue with Facebook

Continue with Google

Continue with Twitter

By continuing, you agree to TikTok's [Terms of Service](#) and confirm that you have read TikTok's [Privacy Policy](#).

Already have an account? [Log in](#)

TikTok.com

Categorization of scope attributes (personal user data)

Data category	Google	Facebook	Apple	LinkedIn
Basic (online identifier)	email (address) <i>profile</i> openid	email (address) <i>public_profile</i>	email (address) name (as given by user)	r_emailaddress name profilePicture headline
Identity (real world)	user.birthday.read user.addresses.read* user.gender.read* user.phonenumbers.read*	user_birthday user_hometown user_gender user_age_range instagram_graph_user_profile*		address birthDate phoneNumbers backgroundPicture
Personal	userinfo.profile photoslibrary* fitness* tasks*	user_location user_photos user_videos instagram_graph_user_media*		geoLocation
Interests	games* user.organization.read*	user_likes user_posts user_link		organizations positions educations projects certifications skills volunteeringInterests volunteeringExperiences
Other Sensitive	contacts drive gmail (email content) documents* spreadsheets* youtube*	user_friends		websites industryName courses testScores summary

*Data not requested (but available) by any site in our dataset.

Categorization of scope attributes (personal user data)

Data category	Google	Facebook	Apple	LinkedIn
Minimum information (basic)	Basic (online identifier)	email (address) <i>profile</i> openid	email (address) <i>public_profile</i>	email (address) name (as given by user) r_emailaddress name profilePicture headline
Potentially private information (non-basic)	Identity (real world)	user.birthday.read user.addresses.read* user.gender.read* user.phonenumbers.read*	user_birthday user_hometown user_gender user_age_range instagram_graph_user_profile*	address birthDate phoneNumbers backgroundPicture
	Personal	userinfo.profile photoslibrary* fitness* tasks*	user_location user_photos user_videos instagram_graph_user_media*	geoLocation
	Interests	games* user.organization.read*	user_likes user_posts user_link	organizations positions educations projects certifications skills volunteeringInterests volunteeringExperiences
	Other Sensitive	contacts drive gmail (email content) documents* spreadsheets* youtube*	user_friends	websites industryName courses testScores summary

*Data not requested (but available) by any site in our dataset.

RPs in US with 2+ non-basic attributes requested

Relying Party	F basic	F user_hometown	F user_location	F user_likes	F user_gender	F user_birthday	F user_friends	F user_photos	F user_video	F user_posts	G basic	G userinfo.profile	A basic	L basic	L r_fullprofile
aliexpress.com	•	•	•		•	•					•				
nba.com *	•			•		•	•								
tripadvisor.com *†	•	•	•	•			•	•			•				
airbnb.com	•	•	•	•		•	•				•		•		
dailymotion.com *†	•				•	•					•				
groupon.com *†	•	•					•				•				
pinterest.com *†	•			•		•	•				•				
glassdoor.com *	•		•			•					•		•		
imdb.com	•				•	•					•		•		
fiverr.com *†	•			•		•					•		•		
gofundme.com *	•						•	•							
yelp.com *†	•				•	•					•	•	•		
autotrader.com	•						•	•					•		
foodnetwork.com	•						•	•			•		•		
hootsuite.com	•						•	•	•	•	•		•		
soundcloud.com	•					•					•	•	•		
slideshare.net *	•						•							•	•

RPs using client-side OAuth flows are shown with *Facebook; †Google
 IdP: (F)acebook, (G)oogle, (A)pple and (L)inkedIn

RPs in US with 2+ non-basic attributes requested

Relying Party	F basic	F user_hometown	F user_location	F user_likes	F user_gender	F user_birthday	F user_friends	F user_photos	F user_video	F user_posts	G basic	G userinfo.profile	A basic	L basic	L r_fullprofile
aliexpress.com	•	•	•		•	•					•				
nba.com *	•			•		•	•								
tripadvisor.com *†	•	•	•	•			•	•			•				
airbnb.com	•	•	•	•		•	•				•		•		
dailymotion.com *†	•				•	•					•				
groupon.com *†	•	•					•				•				
pinterest.com *†	•			•		•	•				•				
glassdoor.com *	•		•			•					•		•		
imdb.com	•				•	•					•		•		
fiverr.com *†	•			•		•					•		•		
gofundme.com *	•						•	•							
yelp.com *†	•				•	•					•	•	•		
autotrader.com	•						•	•					•		
foodnetwork.com	•						•	•			•		•		
hootsuite.com	•							•	•	•	•		•		
soundcloud.com	•					•					•	•	•		
slideshare.net *	•						•							•	•

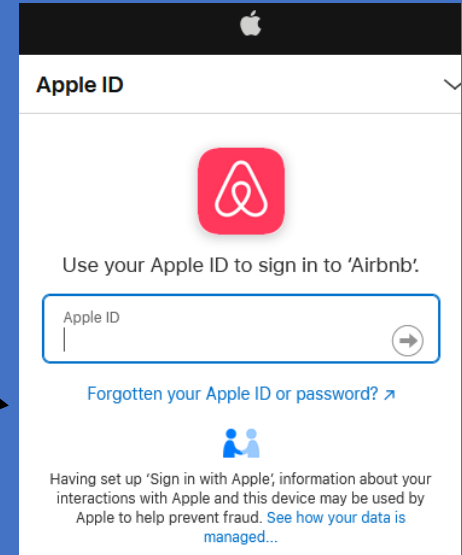
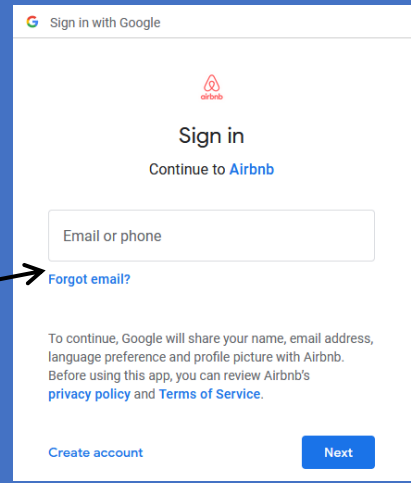
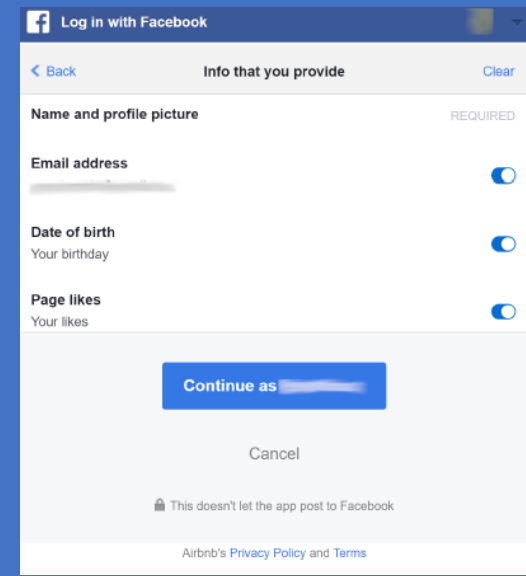
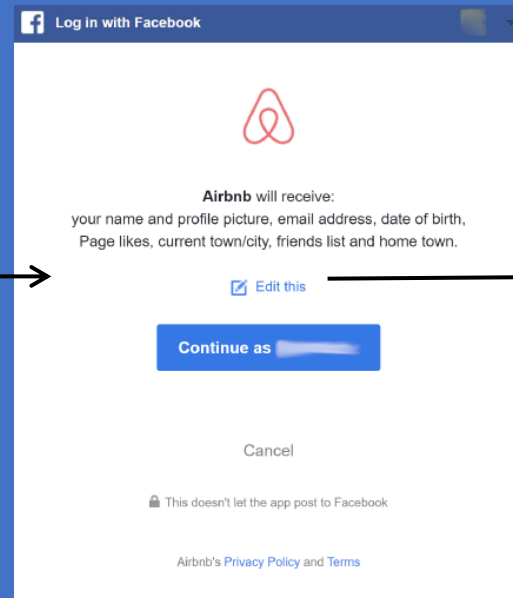
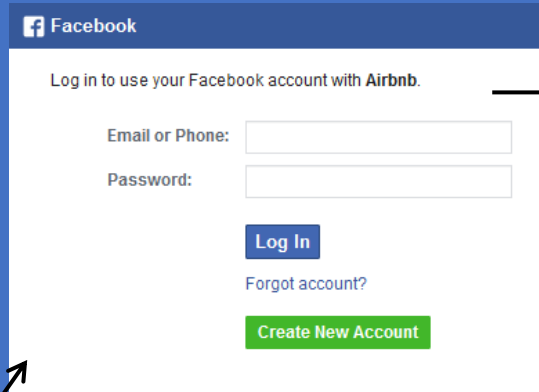
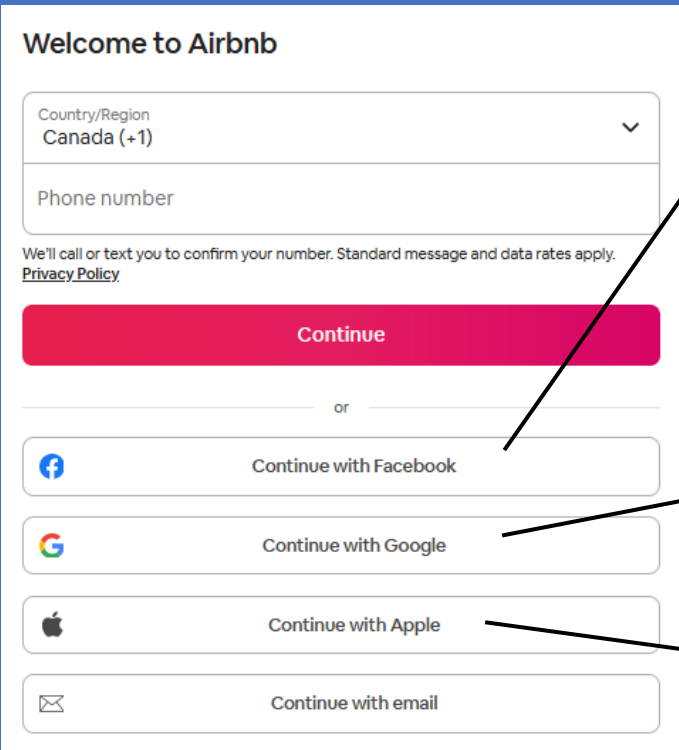
RPs using client-side OAuth flows are shown with *Facebook; †Google
 IdP: (F)acebook, (G)oogle, (A)pple and (L)inkedIn

Considerable privacy variations across IdP choices

- We found 146 of the 184 RPs in US supporting 2+ IdP choices
- Out of 146 RPs, 43 request different categories of data across the IdP choices
 - 42 (out of 43) RPs have an IdP choice that requests only *basic* data
- Possible dark patterns where earlier options request more data
 - 30 (out of 43) RPs with less privacy-friendly choices listed first
- Sites request more data with Facebook as IdP than other IdPs

What are the privacy implications
for end-users?

Users can't compare requested data unless they login with each option



Privacy implications for end-users

- Due to lack of comparative information on IdP choices, users might make privacy-unfriendly choices
 - It could help users if they can see requested attributes before signing in.
- Indicating to users when recommended security practices are followed
 - e.g., a padlock icon when PKCE flow is used.
- Are dark pattern designs being used in OAuth systems?

Ideas for improving end-user privacy in OAuth logins

Standardized descriptions (UI) in login pages


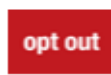
- To be informed, users may need to be aware of what information is shared to RPs and how it is used
- Consistent descriptions for user data attributes across IdP choices
 - e.g., when a RP requests contact lists from Google and Facebook
- Display of comparative information could help users choose from multiple login options
 - Consistent format could help users understand privacy implications
- Standardizing (and showing comparative information) might discourage use of dark pattern designs

Example of a type of standardized UI

Bell Group

information we collect	ways we use your information				information sharing	
	to provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt in			opt out	
cookies						
demographic information		opt in			opt out	
your preferences						
purchasing information		opt in			opt out	
your activity on this site		opt in			opt out	

- Shows what information is collected and how it is used and/or shared with other parties
- Describes access controls available for users to opt in or opt out

	we will collect and use your information in this way		we will not collect and use your information in this way
	by default, we will collect and use your information in this way unless you tell us not to by opting out		by default, we will not collect and use your information in this way unless you allow us to by opting in

The above image shows an example of Privacy Nutrition Labels (CUPS lab)

Source: <https://cups.cs.cmu.edu/privacylabel-05-2009/current/1.php>

Example: Apple's privacy label for Music app

App Privacy

[See Details](#)

The developer, Apple, indicated that the app's privacy practices may include handling of data as described below. For more information, see the [developer's privacy policy](#).

The screenshot displays two columns of data categories. The left column, titled 'Data Linked to You', lists: Purchases, Financial Info, Location, Contact Info, User Content, Search History, Identifiers, Usage Data, and Diagnostics. The right column, titled 'Data Not Linked to You', lists: Diagnostics and Other Data. Each category is accompanied by a small icon representing the data type.

- Shows what information is shared with the app and how it is used
- Uses a consistent format for listing the data collected

Source: <https://www.apple.com/ca/privacy/labels/>

Other ideas...

- Browser extension to provide comparative information when users choose an IdP login
 - Conveying about user data requested via each choice
- Community effort to gather information about RP privacy (crowd-sourced reputation system)
 - e.g., <https://2fa.directory/> (list of sites that support 2FA)
- Automated tool to provide third-party rating of an RP's privacy practices
 - e.g., <https://themarkup.org/blacklight> (identification of user tracking on websites)

Thank you!

As a user, what information would you like to see in order to make privacy-informed choices in SSO logins?

Do any of our results suggest evidence of dark patterns in use?

Any other ideas for informing privacy-conscious users?

Are any of the things we've discussed worth considering in some future version of the OAuth standard?

Thank you!

As a user, what information would you like to see in order to make privacy-informed choices in SSO logins?

Do any of our results suggest evidence of dark patterns in use?

Any other ideas for informing privacy-conscious users?

Are any of the things we've discussed worth considering in some future version of the OAuth standard?

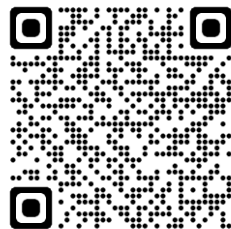
Srivathsan Morkonda Gnanasekaran, Sonia Chiasson, Paul C. van Oorschot

Contact:

SrivathsanMorkonda@cmail.carleton.ca

 <https://www.ccsf.carleton.ca/~smorkonda/>

 <https://www.linkedin.com/in/morkonda/>



OAuth 2.0 and OIDC flows in top 500 sites

Identity Provider	OAuth 2.0 / OIDC Flow	Response Type	Australia			Canada			Germany			India			US		
			N	n	%	N	n	%	N	n	%	N	n	%	N	n	%
Google	Authorization code	code	148	95	64	132	85	64	98	74	76	151	83	55	159	95	60
	Implicit	token	↑	4	3	↑	4	3	↑	0	-	↑	3	2	↑	2	1
		id_token			1		1	1		0	-		0	-		2	1
		id_token token		34	23		35	27		17	17		55	36		50	31
	Hybrid	code id_token	↑	0	-	↑	0	-	↑	0	-	↑	0	-	↑	0	-
		code token		0	-		0	-		0	-		0	-		1	1
		code id_token token		13	9		7	5		7	7		10	7		9	6
Facebook	Authorization code	code	147	102	69	134	90	67	103	73	71	144	82	57	148	84	57
	Implicit	token	↑	4	3	↑	5	4	↑	0	-	↑	2	1	↑	3	2
		token signed_request		41	28		39	29		30	29		60	42		61	41
Apple	Authorization code	code	70	34	49	64	30	47	47	30	64	42	16	38	85	35	41
	Hybrid	code id_token	↑	36	51	↑	34	53	↑	17	36	↑	26	62	↑	50	59
LinkedIn	Authorization code	code	9	9	100	11	11	100	3	3	100	10	10	100	11	11	100

$$\% = n/N * 100$$

N: # of top 500 sites offering the SSO option
n: # of sites using the given flow

RPs in US with 2+ IdP options
 (in the order showed on RP site)

Relying Party	Option 1	Option 2	Option 3
aliexpress.com	F b i p - -	G b - - - -	- - - - -
feedly.com	G b - p - -	F b - - - -	A b - - - -
hootsuite.com	F b - p n -	G b - - - -	A b - - - -
offerup.com	F b - - - s	G b - - - -	A b - - - -
poshmark.com	F b - - - s	A b - - - -	G b - - - -
quizlet.com	G b - - - -	F b i - - -	A b - - - -
slickdeals.net	F b - - - -	G b - p - -	- - - - -
soundcloud.com	F b i - - -	G b - p - -	A b - - - -
vimeo.com	F b - - - -	G b - p - -	A b - - - -
wordpress.com	G b - p - -	A b - - - -	- - - - -
airbnb.com	F b i p n s	G b - - - -	A b - - - -
allrecipes.com	F b - - - s	G b - - - -	- - - - -
autotrader.com	F b - p - s	A b - - - -	- - - - -
blizzard.com	F b - - - s	G b - - - -	A b - - - -
canva.com	G b - p - -	F b - - - -	A b - - - -
chess.com	F b - - - -	G b - p - -	A b - - - -
coursera.org	G b - - - -	F b i - - s	A b - - - -
dailymotion.com	F b i - - -	G b - - - -	- - - - -
desmos.com	G b - p - -	A b - - - -	- - - - -
dropbox.com	G b - - - s	A b - - - -	- - - - -
epicgames.com	F b - - - s	G b - - - -	A b - - - -
expedia.com	A b - - - -	F b - - - -	G b - p - -
fiverr.com	F b i - n -	G b - - - -	A b - - - -
foodnetwork.com	A b - - - -	F b - p - s	G b - - - -
gamespot.com	F b - - - -	G b - p - -	- - - - -
glassdoor.com	F b i p - -	G b - - - -	A b - - - -
goodreads.com	F b - - - s	G b - - - -	A b - - - -
groupon.com	F b i - - s	G b - - - -	- - - - -
houzz.com	F b - - - s	G b - - - -	A b - - - -
imdb.com	F b i - - -	G b - - - -	A b - - - -
kickstarter.com	A b - - - -	F b - - - s	- - - - -
loom.com	G b - p - -	A b - - - -	- - - - -
meetup.com	F b - - - s	G b - - - -	A b - - - -
pinterest.com	F b i - n s	G b - - - -	- - - - -
rakuten.com	G b - - - s	F b - - - -	A b - - - -
slideshare.net	L b i p n s	F b - - - s	- - - - -
smartsheet.com	G b - p - -	A b - - - -	- - - - -
theatlantic.com	F b i - - -	G b - - - -	- - - - -
timeanddate.com	F b - - - -	G b - p - -	- - - - -
tripadvisor.com	G b - - - -	F b i p n s	- - - - -
trulia.com	F b - p - -	G b - - - -	- - - - -
ultimate-guitar.com	G b - p - -	F b - - - -	A b - - - -
yelp.com	F b i - - -	G b - p - -	A b - - - -