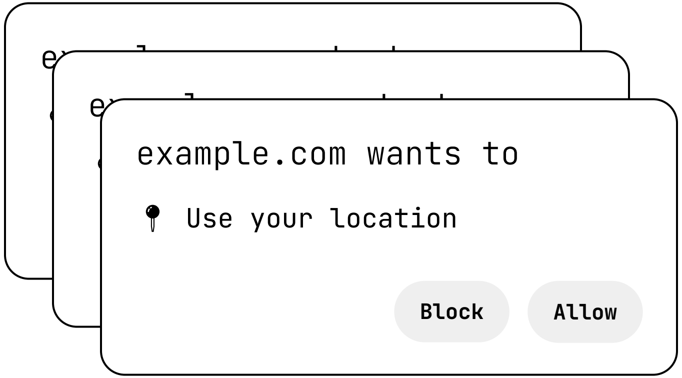
LOOK!NG BEYOND PERMISSION PROMPTS

NA CHEN ✴ IXD @ GOOGLE CHROME ✴ SERENA CHEN ✴ IXD @ GOOGLE CHROME ✴ SERENA CHEN ✴ IXD @ GOOGLE CHR

SENIX ✴ PRIVACY ENGINEERING PRACTICE & RESPECT ✴ SEP 2023 ✴ USENIX ✴ PRIVACY ENGINEERING PRACTICE & RES

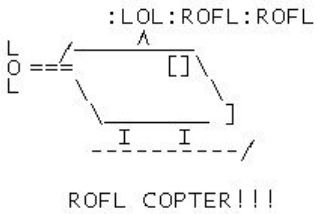
- serena
- ux designer
- google chrome
- pronounces it “owned” not “poned”



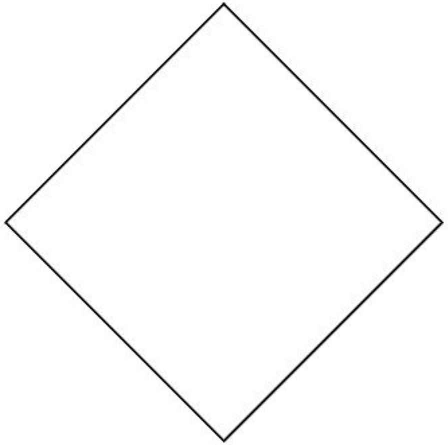
example.com wants to

📍 Use your location

1.
THE POINT OF PROMPTS



In the beginning, the web was for documents.



Over time, we added more capabilities.

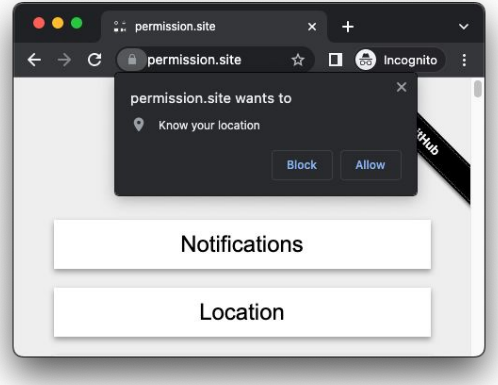
example.com wants to

🎤 Use your microphone

Block
Allow

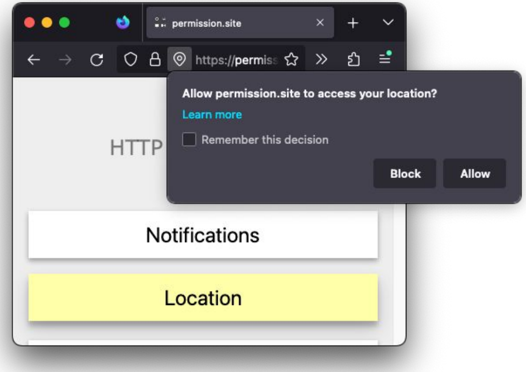
The permission prompt is to make sure you actually intend to let the website use a new capability.

Permissions are for detecting user *intent*



permission.site wants to

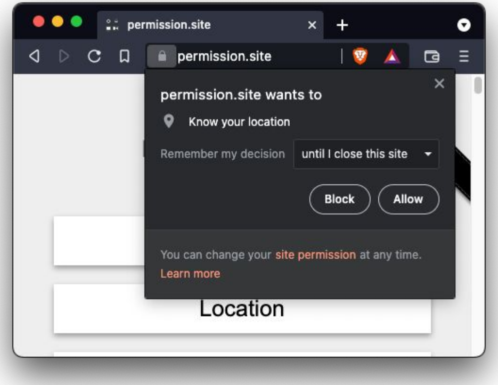
Know your location



Allow permission.site to access your location?

Learn more

□ Remember this decision

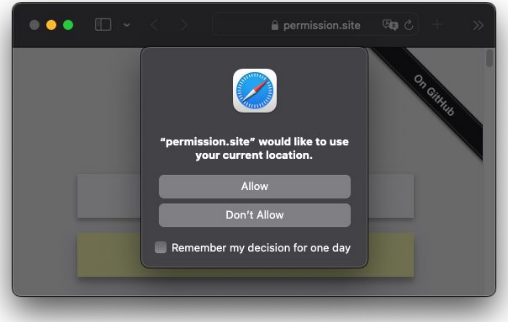


permission.site wants to

Know your location

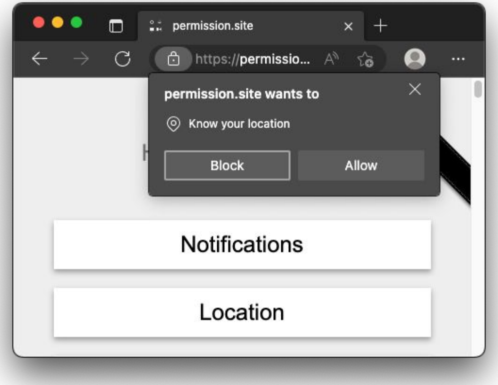
Remember my decision: until I close this site

You can change your site permission at any time. Learn more



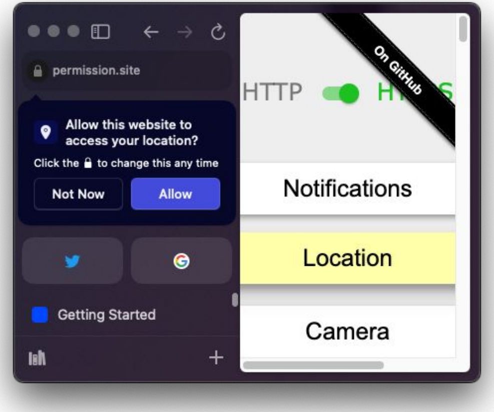
“permission.site” would like to use your current location.

□ Remember my decision for one day



permission.site wants to

Know your location

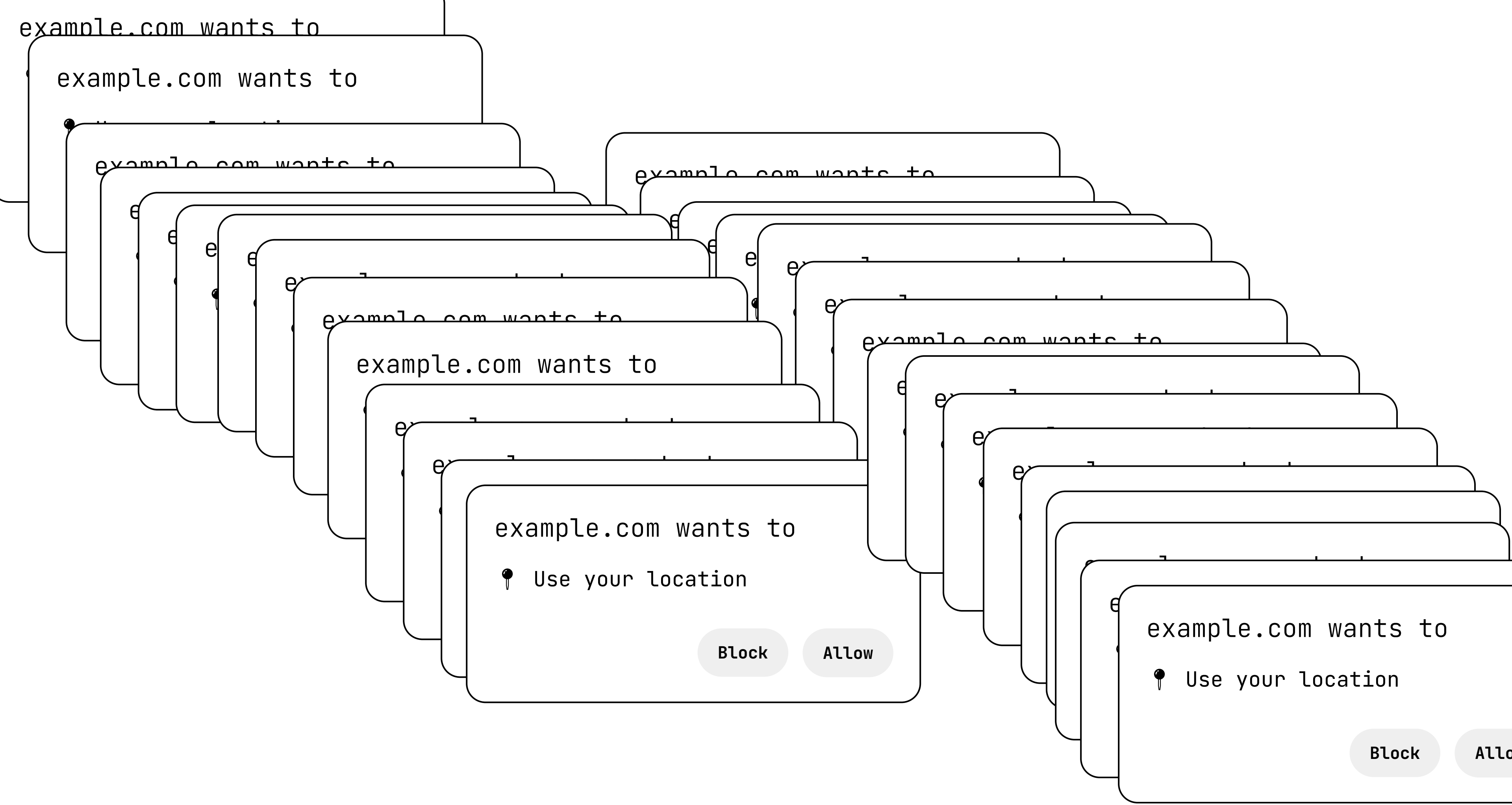


Allow this website to access your location?

Click the 🔒 to change this any time

Q: Did you have a nice experience?

A: no


example.com wants to
Use your location
Block
Allow
example.com wants to
Use your location
Block
Allo

The current way we handle permissions *does not scale.*

2.

MO’ PROMPTS MO’ PROBLEMS

serena’s list of gripes 😤

1. Prompts are interruptive

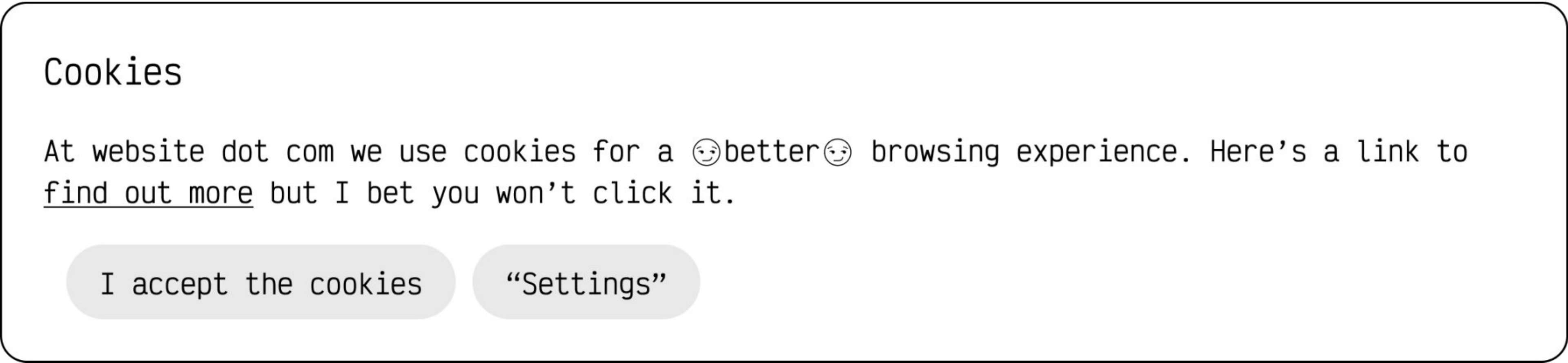
    ⇢ Timing is controlled by the site, not by the user

    ⇢ Often appears immediately on page load

    ⇢ People don’t have enough context to make a decision

serena’s list of gripes 😤

1. Prompts are interruptive
2. Prompts are repetitive
   - ⇢ Your prompt is not the only one!



Cookies

At website dot com we use cookies for a 😏better😏 browsing experience. Here’s a link to find out more but I bet you won’t click it.

serena’s list of

1. Prompts are int

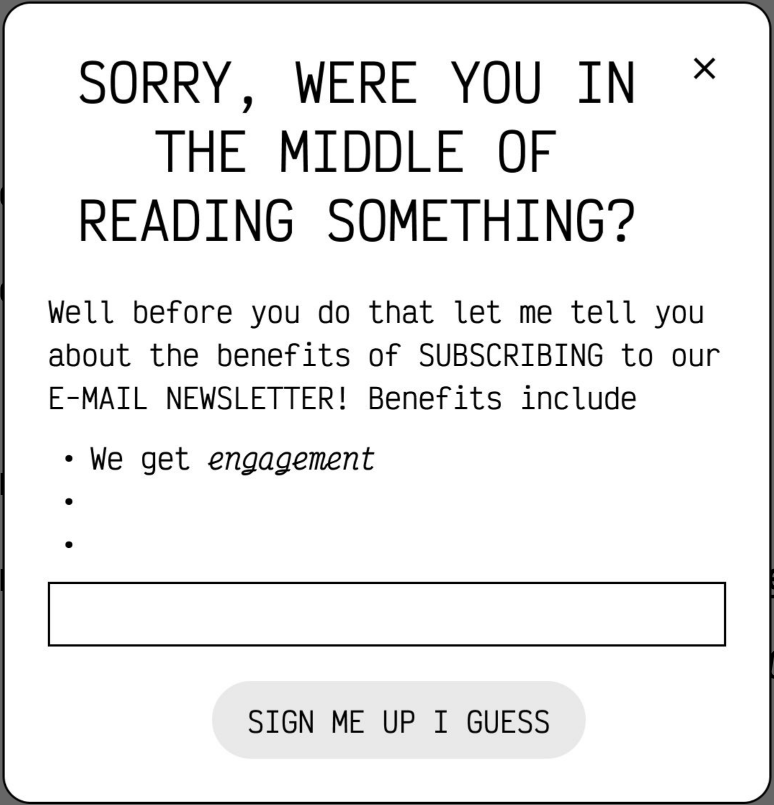
2. Prompts are rep

   ⇢ Your prompt

   ⇢ We are addi

   ⇢ Interruptio g

Click Anything™



SORRY, WERE YOU IN THE MIDDLE OF READING SOMETHING?

Well before you do that let me tell you about the benefits of SUBSCRIBING to our E-MAIL NEWSLETTER! Benefits include

- We get *engagement*
-
-

serena’s list of gripes 😤

1. Prompts are interruptive
2. Prompts are repetitive
    - Your prompt is not the only one!
    - We are adding more capabilities still
    - Interruptions and repetitions → ~~Satisficing~~
      Panic And Click Anything™

serena’s list of gripes 😤

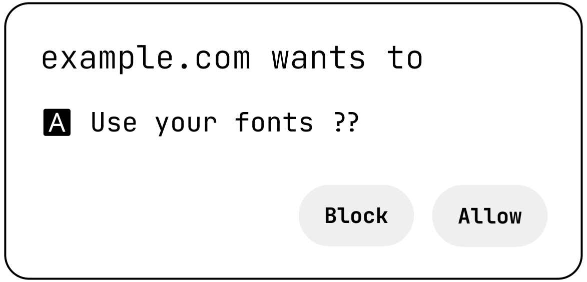
1. Prompts are interruptive

2. Prompts are repetitive

3. Risks are hard to explain

    - I don’t know what a “”web serial”” is and at this point I’m too afraid to ask

    - Imagine explaining the concept of fingerprinting to someone who is busy with something else



example.com wants to

🅰 Use your fonts ??

EXAMPLE!

Fonts API

A main risk for Fonts API is fingerprinting via the list of installed fonts — not the files themselves.

Imagine explaining that!

serena’s list of gripes 😤

1. Prompts are interruptive
2. Prompts are repetitive
3. Risks are hard to explain

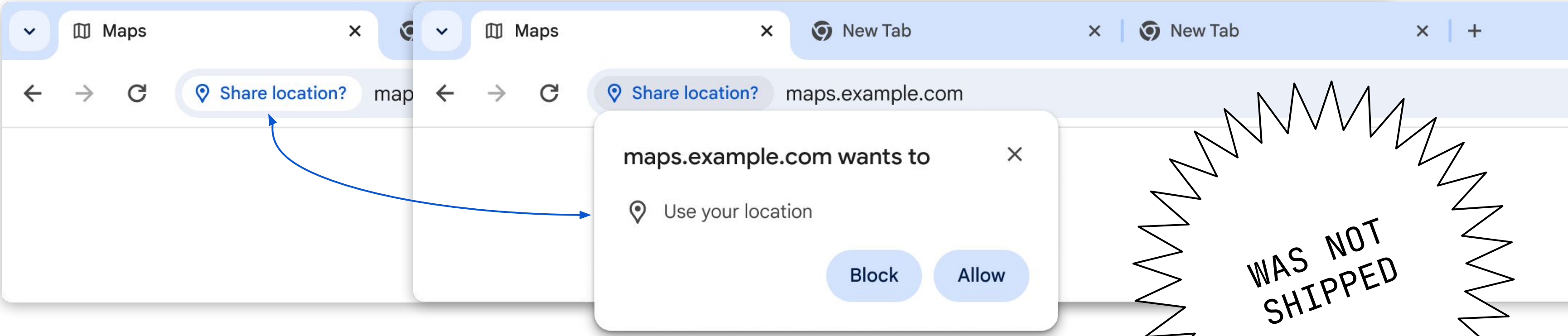
[long, heavy sigh]

3.

THE THINGS WE TRIED

Oh, prompts are interruptive?

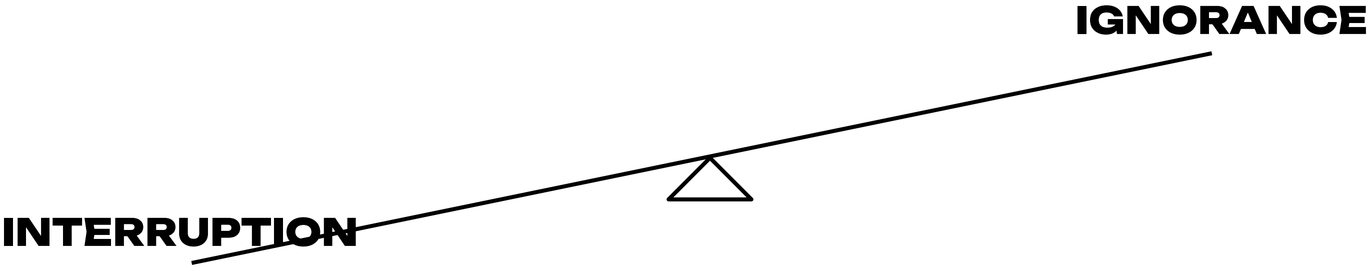
- Introducing: the permission request chip
  - Out of the way
  - Grant rates dropped from 20% to less than 1%



maps.example.com wants to

Use your location

WAS NOT SHIPPED

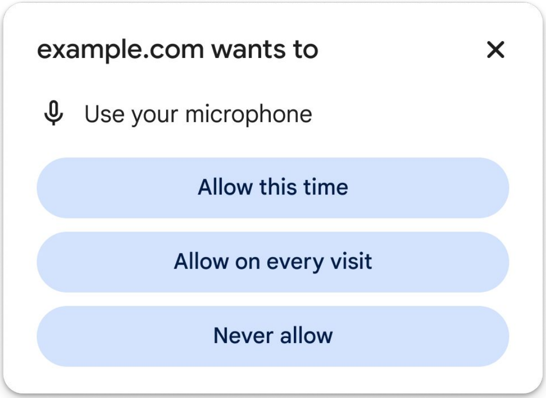


IGNORANCE

INTERRUPTION

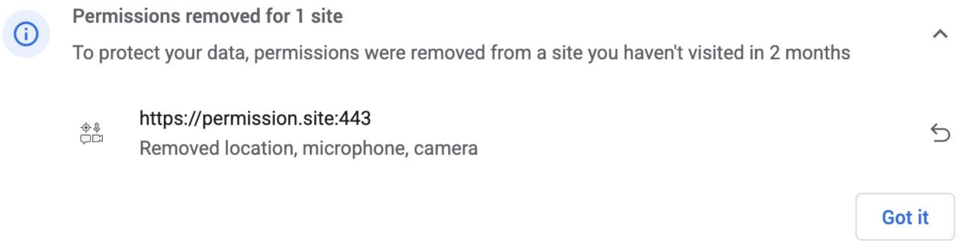
Oh, risks are hard to explain?

- ✴ Automatic permission revocation
- ✴ One-time grants



example.com wants to

Use your microphone



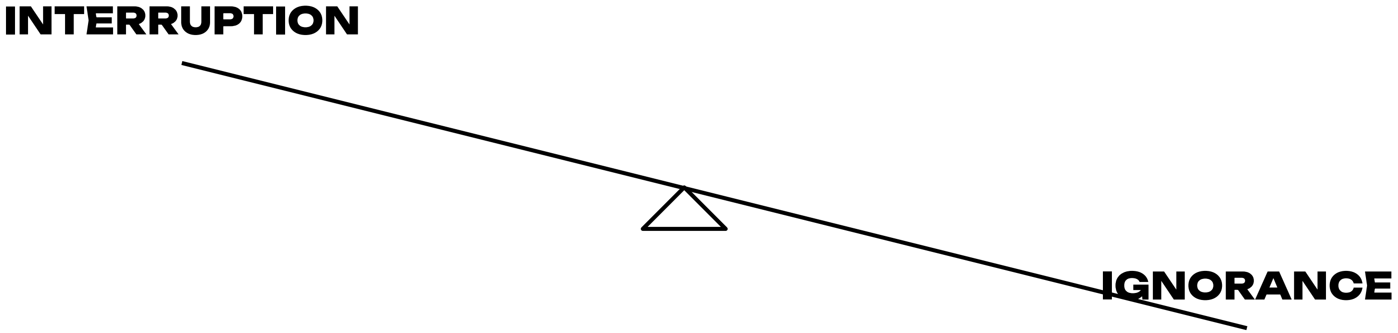
Permissions removed for 1 site

To protect your data, permissions were removed from a site you haven't visited in 2 months

https://permission.site:443

Removed location, microphone, camera

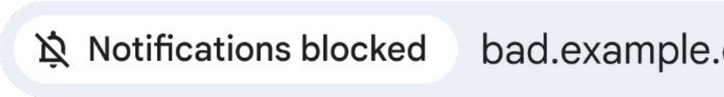
SHIPPED!



INTERRUPTION

IGNORANCE

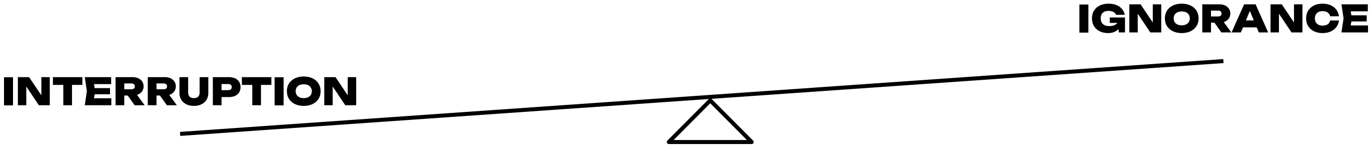
Oh, there's too many prompts?



- Hide what people don't want
  - Based on user behaviour (settings opt-in, repeated denials)
  - Based on site behaviour (high-prompt/low-grant sites)
- Chrome Permission Suggestion Service (CPSS)
  - On-device, privacy-preserving ML that predicts likelihood of user grant
  - *If* highly confident (>95% precision) user will not grant, we show the chip UI

SHIPPED!

Bilogrevic et al. ["Shhh...be quiet!" Reducing the Unwanted Interruptions of Notification Permission Prompts on Chrome.]() USENIX Security, 2021.

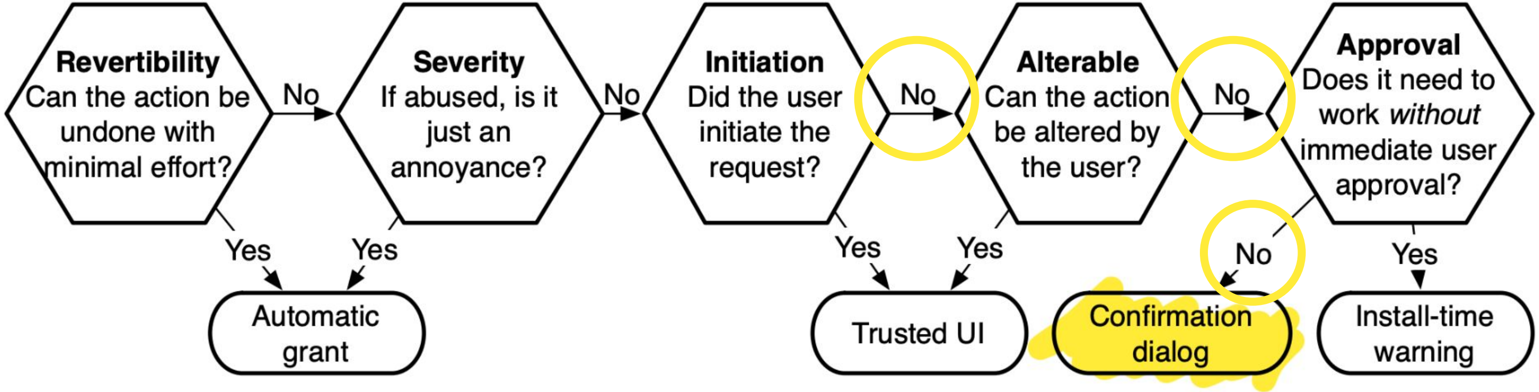


INTERRUPTION

IGNORANCE

4.

THE DEEPER PROBLEM


Revertibility
Can the action be undone with minimal effort?
No
Yes
Severity
If abused, is it just an annoyance?
No
Yes
Automatic grant
Initiation
Did the user initiate the request?
No
Yes
Alterable
Can the action be altered by the user?
No
Yes
Trusted UI
Approval
Does it need to work *without* immediate user approval?
No
Yes
Confirmation dialog
Install-time warning

Why is the user only brought in at the end?

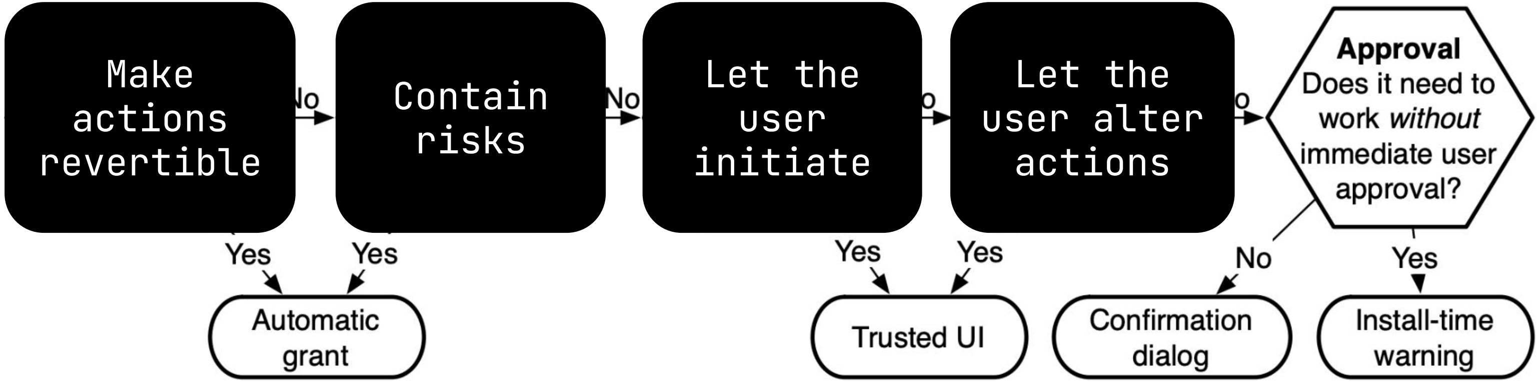
Felt, A. P. (2012). Towards Comprehensible and Effective Permission Systems

How web APIs work

1. Website tries to use a capability
2. Browser checks for permission
3. If no permission → pop prompt
   - ⇢ At *no point* before this does the user need to be involved!

“Developer-push”

How we currently design software to handle permissions is a “developer-push” model.



Felt, A. P. (2012). Towards Comprehensible and Effective Permission Systems

GOAL:

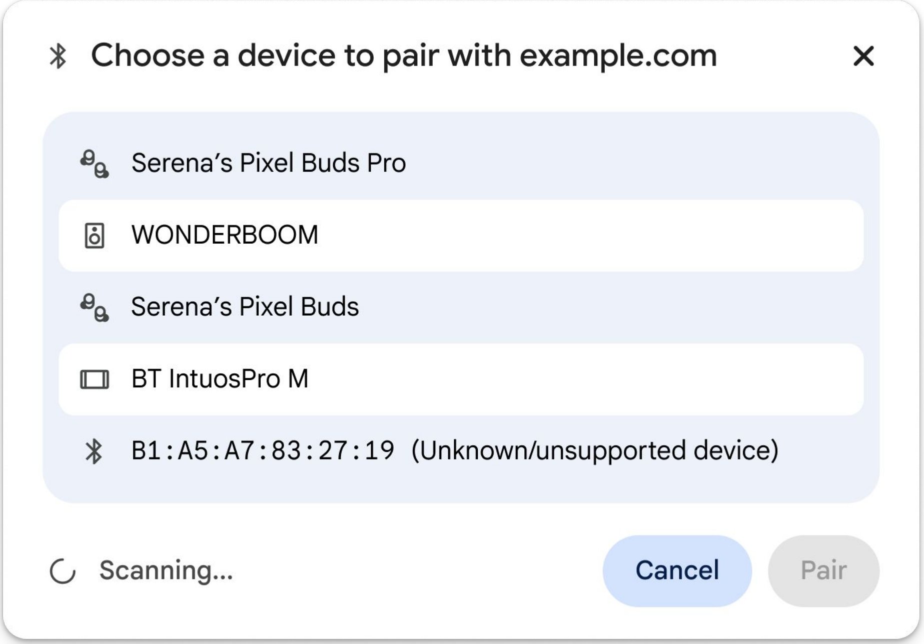
Detect user intent

5.
BEYOND PROMPTS

5 concepts

- User selection
- Piggyback off known concepts
- Sandbox risks
- Direct controls
- Embed triggers

User selection



Choose a device to pair with example.com

Serena’s Pixel Buds Pro

WONDERBOOM

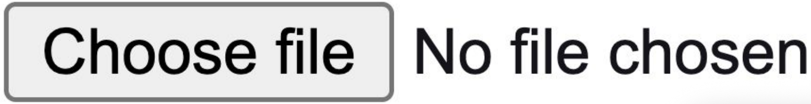
Serena’s Pixel Buds

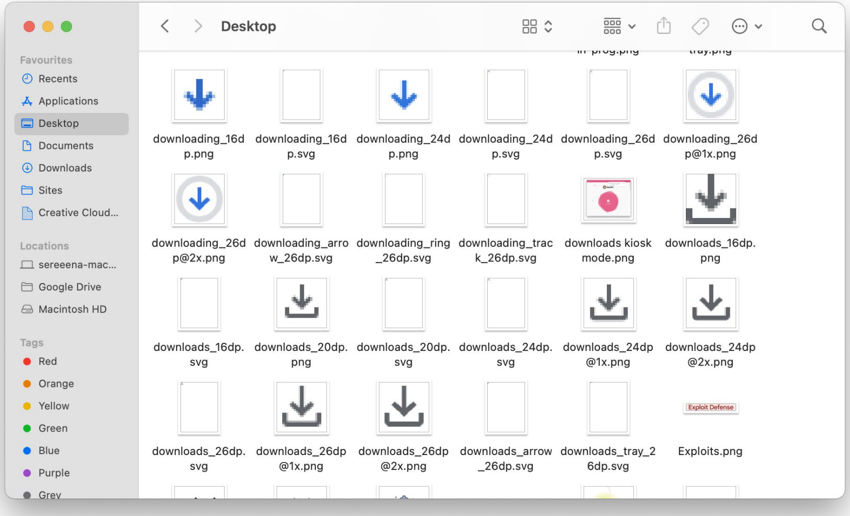
BT IntuosPro M

B1:A5:A7:83:27:19 (Unknown/unsupported device)

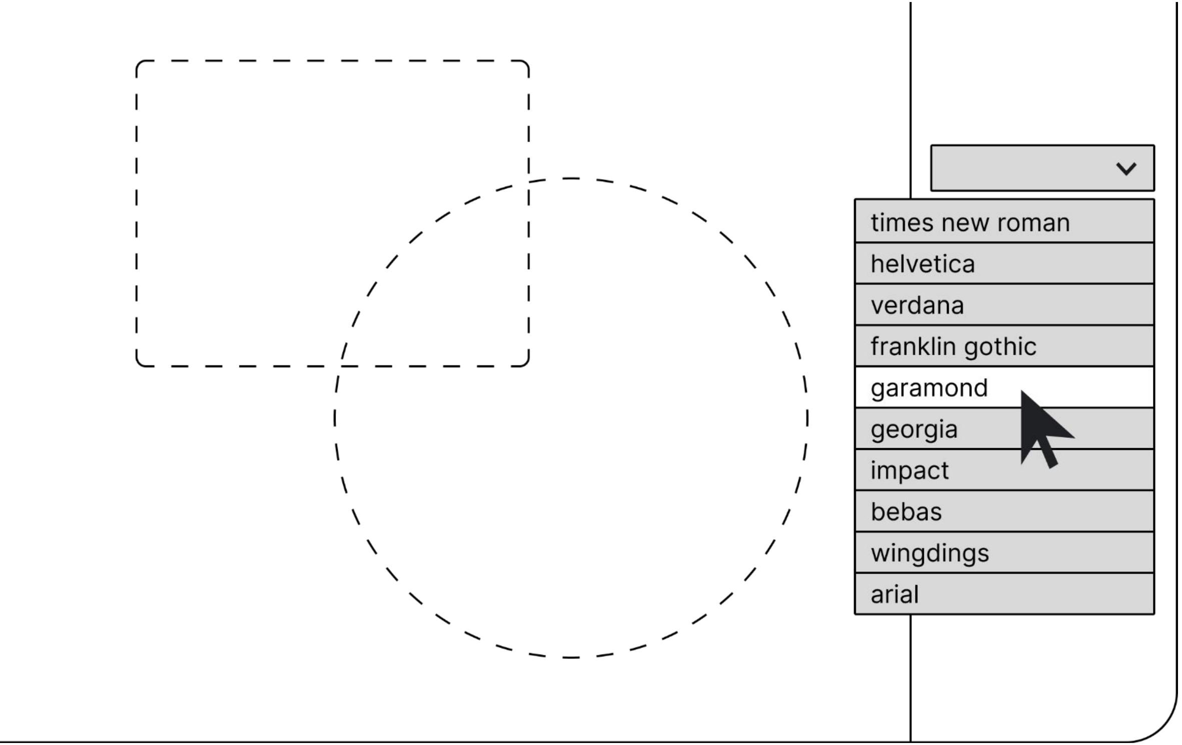
Scanning...

Known concepts

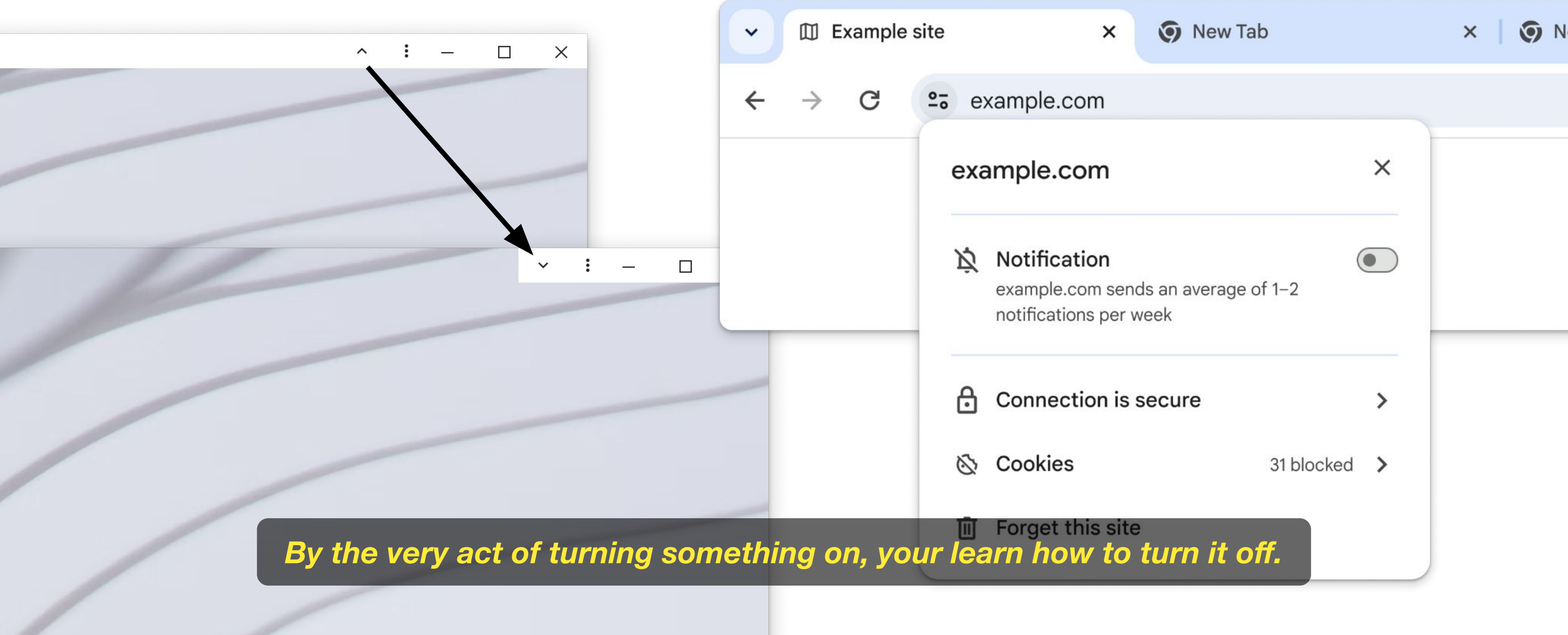




Sandbox risks



Direct controls



example.com

Notification

example.com sends an average of 1–2 notifications per week

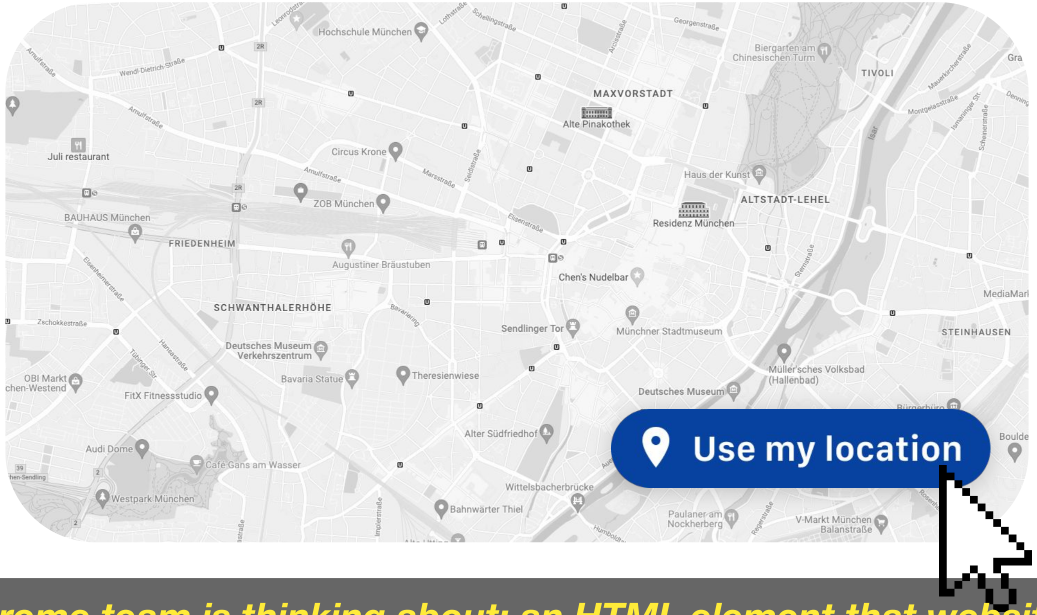
Connection is secure

Cookies 31 blocked

Forget this site

By the very act of turning something on, your learn how to turn it off.

Embed triggers



Something the Chrome team is thinking about: an HTML element that websites can use on their pages to let people "pull" on the capabilities they want, they they choose and are ready for it.

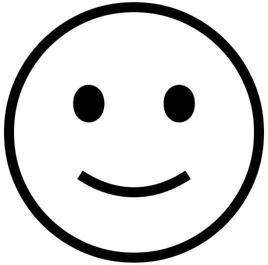
6.

TO THINK OUTSIDE THE BOX WE MIGHT NEED BIGGER BOXES

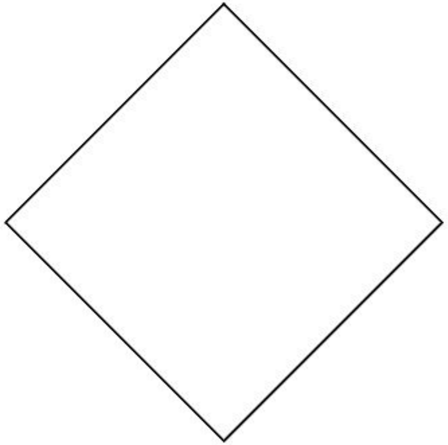
What did we learn on the show today?

1. Permissions are for detecting user intent
2. Prompts do not scale
3. Solutions so far seesaw between interruption & ignorance
4. We need user signals earlier in the interaction flow
5. Five concepts beyond just prompting

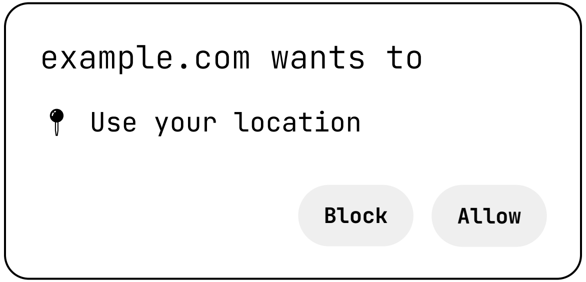
From *developer-push* to *user-pull*



We can design permission moments directly into the natural flow of using something.



This allows us to enable a more powerful web without sacrificing usability, security or privacy.



example.com wants to

📍 Use your location

By adding new ideas to our toolkit, we can take some pressure off the humble permission prompt.

THANKS!

Further reading—

”Shhh...be quiet!” Reducing the Unwanted Interruptions of Notification Permission Prompts on Chrome. USENIX Security, 2021.
Report for the W3C Workshop on Web Permissions, Munich, Germany, 2022.