

# Permission Misuse & **Dark Patterns**

W3C Permissions Workshop, Dec 5, 2022

Balazs Engedy, Igor Bilogrevic, Google

# Goals for this session

Enumerate dark patterns w/permission UX

Discuss why they work

Discuss how we make them not work

# Anti-pattern vs. dark pattern

**“Anti-pattern”** Pattern that might seem good at a first glance, but has less obvious negative implications, and thus should be avoided.


**“Dark pattern”** Pattern for tricking users into performing unintended/unwanted actions through misleading interface design.

**Table 1.** Privacy Strategies vs. Dark Strategies.

---

| <b>Strategies</b> |                        |
|-------------------|------------------------|
| <b>Hoepman</b>    | <b>Dark Strategies</b> |
| MINIMIZE          | MAXIMIZE               |
| HIDE              | PUBLISH                |
| SEPARATE          | CENTRALIZE             |
| AGGREGATE         | PRESERVE               |
| INFORM            | OBSCURE                |
| CONTROL           | DENY                   |
| ENFORCE           | VIOLATE                |
| DEMONSTRATE       | FAKE                   |

---



# Why do dark patterns work? Some hypotheses:

Lack of meaningful controls & choices

Lack of contextual integrity

Developer-centric capabilities

Users underestimate consequences

# One potential framework for mitigations

**Usable Security  
Team**

**Empower the user**

Understanding ----- Friction  
Control ----- Interruption



**API Owner  
Team**

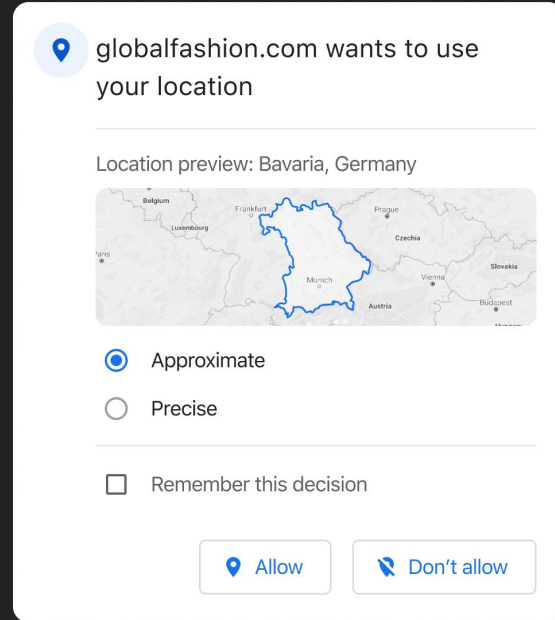
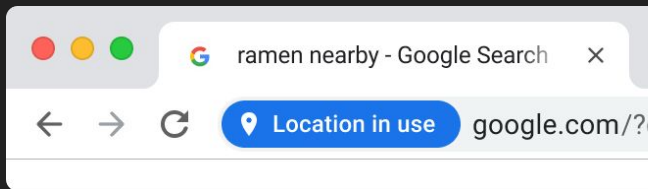
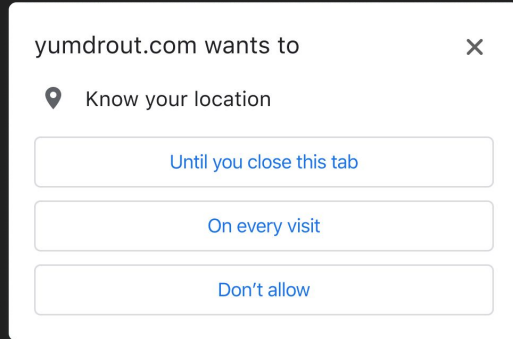
**Change the  
capability**

**Counter-Abuse  
Team**

**Policy based app  
review & enforcement**

~~badsite.url.com~~  
~~verybadsite.evill.com~~  
~~notificationfarmsite.com~~

# Empowering the user – Static UI changes



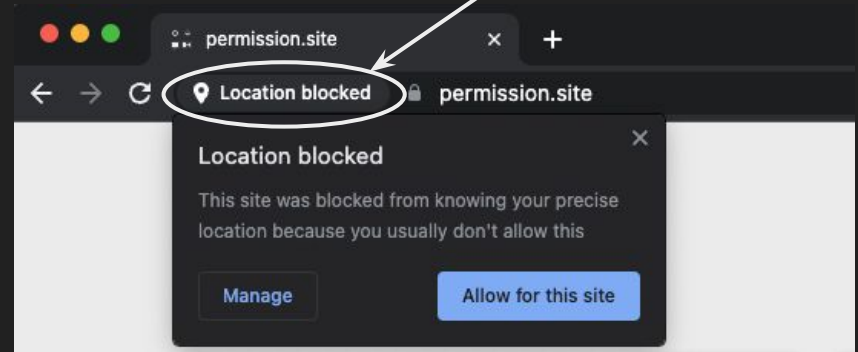
# Empowering the user – Dynamic UI improvements

## Web Permission Predictions

Show quieter prompt when permission is unlikely to be granted

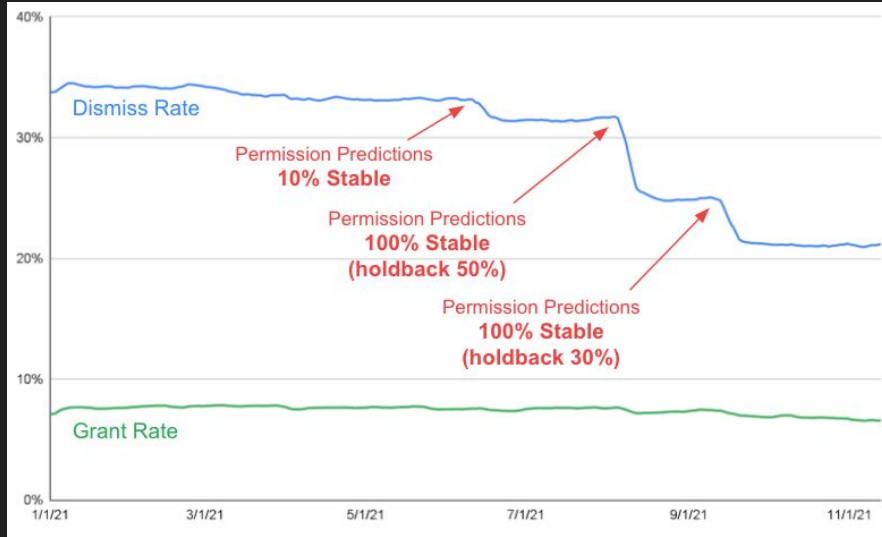
- Reduces interruptions while users remain in control
- Uses on-device ML models (TFLite) for inference at permission request time
- Models are trained on the backend based on Chrome telemetry from users who have it enabled

Initially only this subtle chip is shown. The prompt is only shown if chip is clicked.





# Web Permission Predictions



Possible prompt actions are: Grant, Deny (permanent), Dismiss (temporary), Ignore

## Shipped:

- Server-assisted predictions based on past user decisions for notifications and geolocation
- Moved ML model on-device

## Shipping soon (in H1'23):

- Predictions also based on additional contextual signals