Usable Privacy in Privacy Badger

Bennett Cyphers
Staff Technologist, EFF
bennett@eff.org

Who is EFF?

- Member-funded non-profit organization
- Privacy, free expression, and innovation
- ~40k dues-paying members worldwide

The history of DNT
and the breakdown of diplomacy

A Badger is Born

DNT and the dream of a universal opt-out

- 2009: v1 HTTP DNT standard proposed, implemented
- 2010: FTC calls for universal DNT system
- 2011: W3C working group chartered
- 2011: all major browsers support opt-in DNT signal
- 2012: Digital Advertising Alliance (DAA) makes agreement with White House to honor DNT

DNT and the way dreams die

- Mid 2012: Internet Explorer 10 turns on DNT by default
- Mid 2012: DAA immediately backs out
- Late 2012: Yahoo, Google, others follow
- 2014: EFF introduces Privacy Badger
- ...2018: W3C DNT working group charter expires for the last time, with nothing to show for it

Privacy Badger

- **Goals:**
  - Stop *non-consensual* tracking from third parties
  - Spread awareness about tracking, DNT
  - Promote our idea of DNT compliance
  - Punish trackers who don't respect DNT by blocking them outright
- **Constraints:**
  - Easy to use, cross-platform (limited to WebExtensions APIs)
  - Small dev team
  - No block list allowed

How Privacy Badger works,
and when it doesn't

Where we are

Basic mechanics

- **Send DNT=1 with every third-party request**
  - If a domain posts an acceptable DNT policy, let it do what it wants
  - Otherwise, if it looks like it's tracking, learn to block it
- **Use heuristics to identify trackers**
- **Three strikes and you're out**

Heuristics

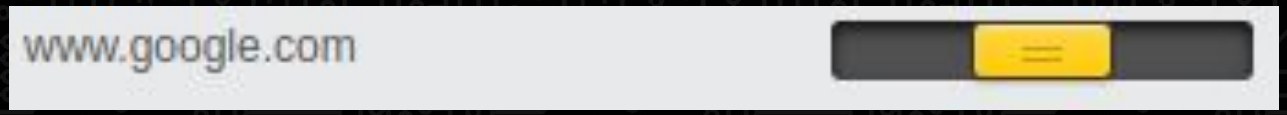
Third party “tracking” actions:

- Cookies with sufficient entropy
- Localstorage writes/reads with sufficient entropy
- Canvas fingerprinting

Compromises

- **Assumptions:**
  - Each TLD+1 is either a tracker or not
  - Blocking third-party trackers *usually* doesn't break a site
- **Workarounds:**
  - Cookie-blocked domains
  - User controls for each third-party domain
  - Widget replacement

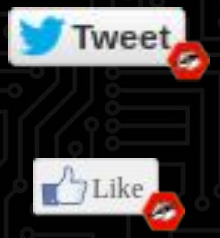
Cookie-blocked domains



- Allowed to make third-party requests
- Not allowed to use localstorage, cookies
- `Referer` header stripped
- Current cookie-block list (“yellowlist”) has 670 domains, unfortunately including Google, Facebook
- Assumption: blocking third-party access to cookies + localstorage *almost never* breaks a site

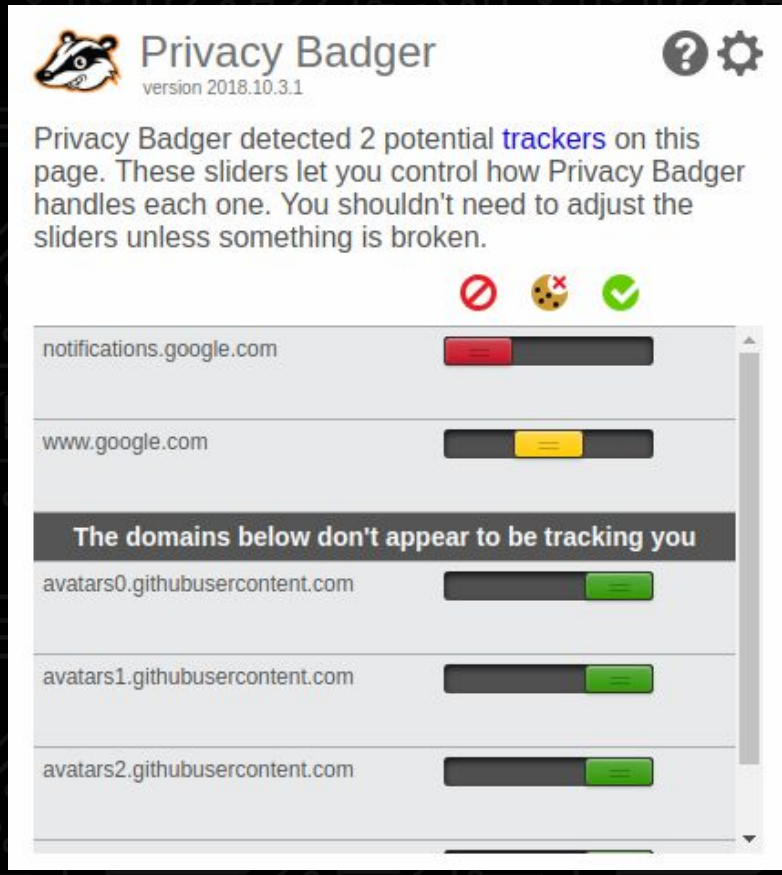
Widget replacement

- Some pages rely on complex plugins that require stateful requests
  - Facebook like button needs cookies
  - Vimeo embedded player needs `referer`
- In these situations, allow the user to opt-in to tracking



User controls

- Users can view and control settings for each domain
- Able to:
  - Permanently allow requests from certain third parties
  - Permanently disable Privacy Badger on certain first parties



Keeping up with user expectations, navigating a changing landscape

Where we're going

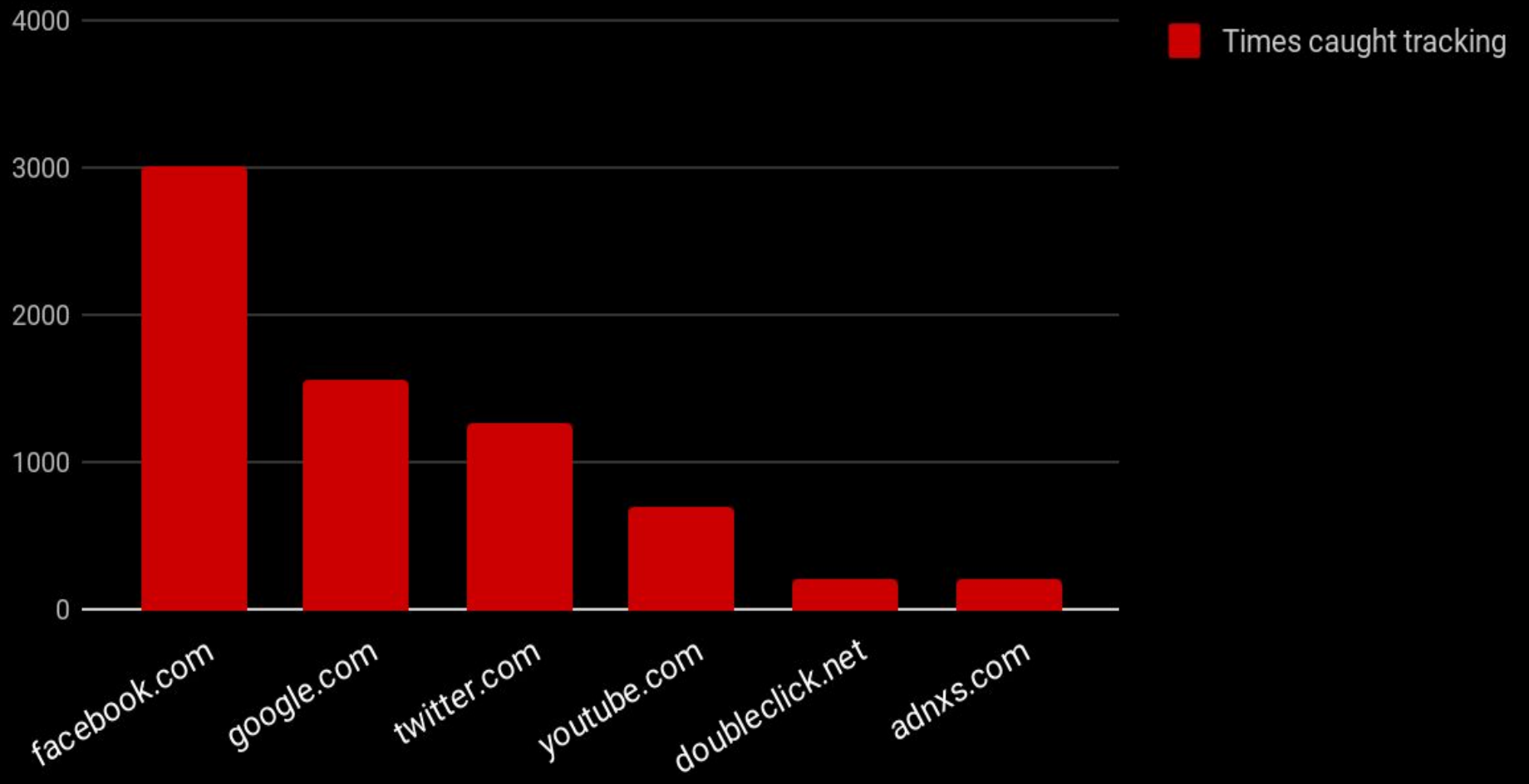
First-party & software-specific features

- Outgoing link tracking
  - unwrap link shims, `<a ping>`
  - Currently active on Facebook, Twitter, Google
- Heuristics for first→third party tracking
  - cookie sharing
  - beacon requests
- Remove tracking URL parameters
  - `utm_*`, `fbclid`
- Fingerprint randomization
- Detect and block screen recorders

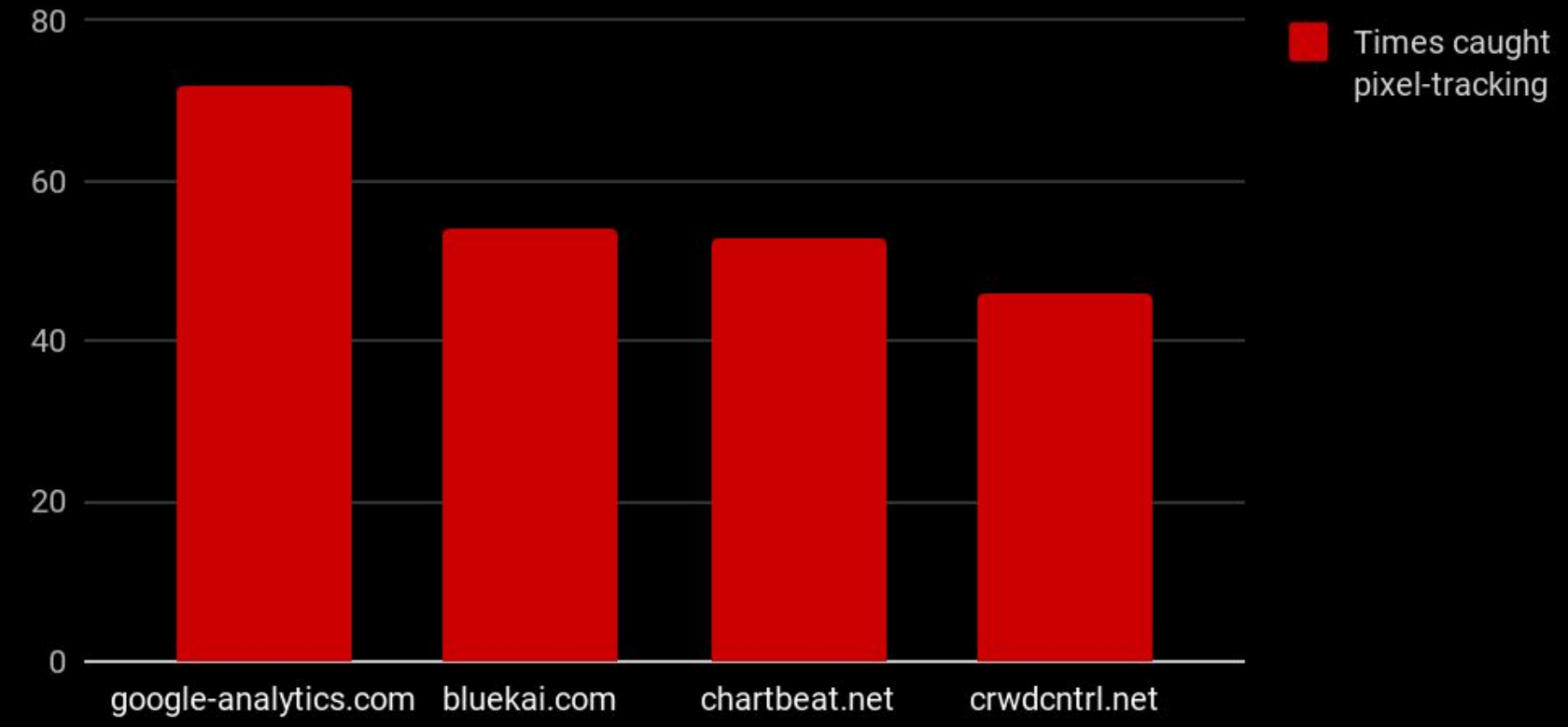
Badger Sett

- Pre-train Privacy Badger on popular sites
- Use Privacy Badger as an observer to survey the web
- Test out new heuristics and measure effectiveness

Most common trackers in top 10,000 sites



Most common cookie-sharing pixel trackers (10k sites)



Privacy Badger Mobile

- The Web is no longer most of the Net
- Trackers in apps are hidden, protected by OS
- How can we detect trackers in proprietary software?
  - APK analysis
  - Client-side software instrumentation
  - Network monitoring significantly less useful
- Domain-based blocking is viable for now. For how long?

Q? A.