The Case for a General and Interaction-based Third-party Cookie Policy

Istemi Ekin Akkus[1], Nicholas Weaver[2]

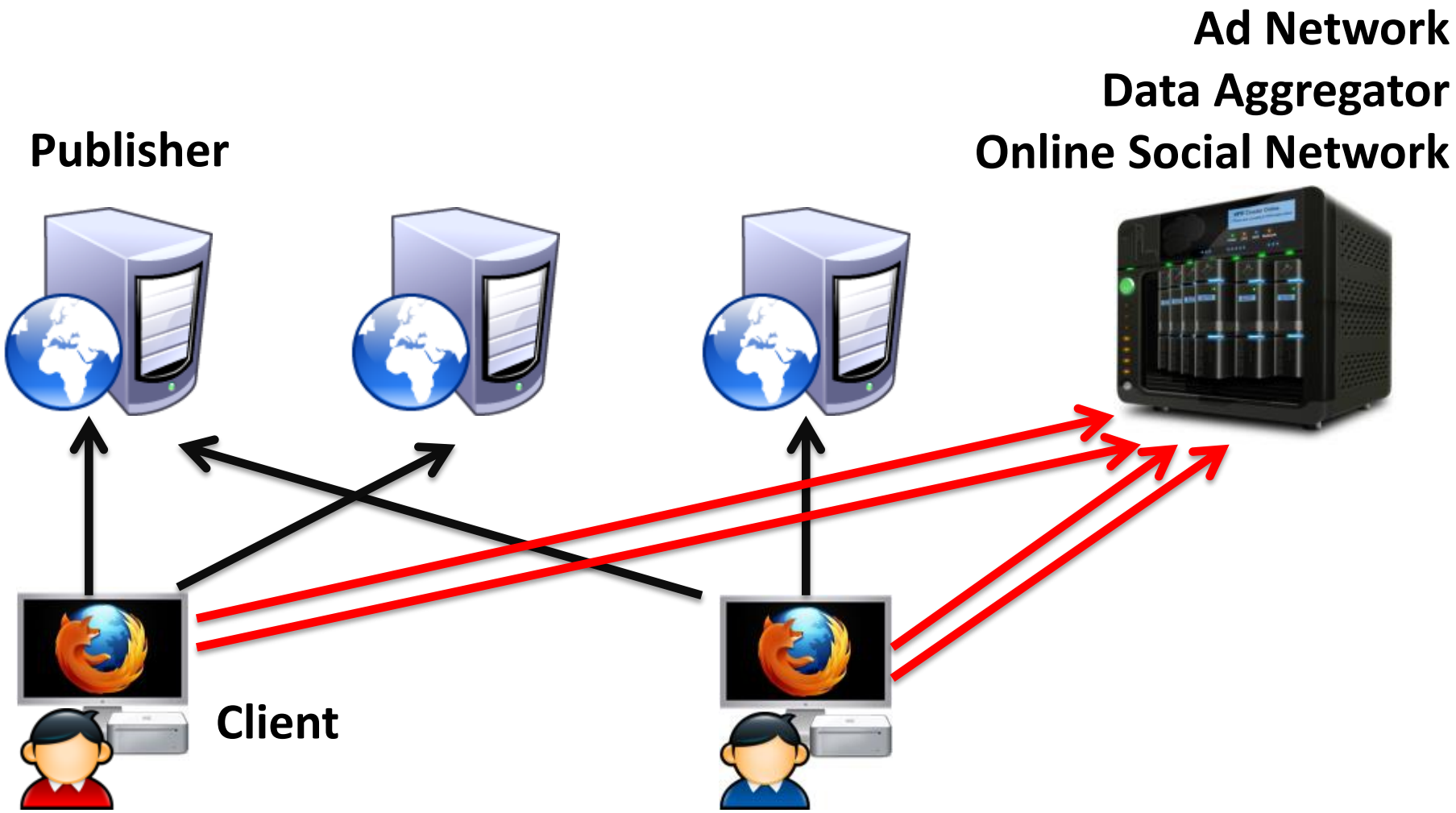
[1] Max Planck Institute for Software Systems (MPI-SWS)

[2] ICSI & UC Berkeley

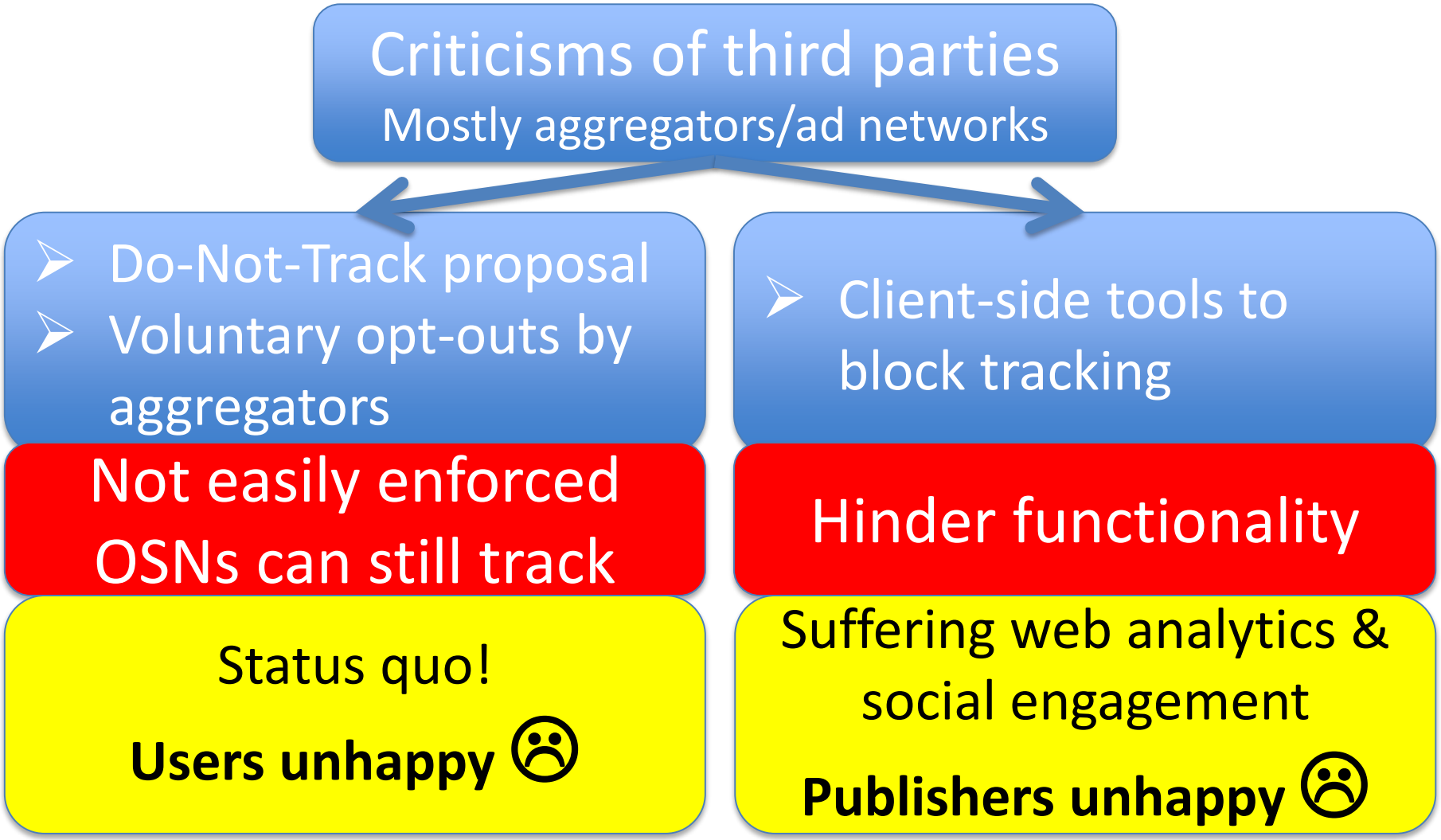
Sample Web Page

- Content
  - Optimized with web analytics
- Advertisements
  - Monetization
- Social widgets
  - Engagement and exposure

Third-party Tracking



Current State of Tracking



Goal

Devise a general cookie policy that

- Prevents third parties from tracking
- Enables social features on-demand
- Does not penalize non-tracking services

Outline

- Assumptions
- Existing approaches and shortcomings
  - Cookie policies
  - Blacklist-based client tools
- Our policy
  - Two-click control
  - Generalization
- Discussion
- Implementation and preliminary evaluation
- Future & ongoing work

Assumptions

- No attempts to circumvent cookie preferences
  - No ‘stateless’ tracking (i.e., fingerprinting)
  - No ‘behind-the-scenes’ cookie synching

➔ Considered frowned upon if not illegal

  - (e.g., Doubleclick vs. Safari)

- Interactive mashups
  - No passive mashups requiring user cookies

Existing Cookie Policies

- Allow all third-party cookies
  - Default policy; allows tracking
- Deny all third-party cookies
  - Prevents tracking
  - Breaks functionality of social widgets
- Allow third-party cookies from 'visited sites'
  - Aimed to prevent tracking by data aggregators, but enable social widgets
  - Allows OSNs to track

Blacklist-based Client Tools

1. Scan the page while loading
2. Check page elements against a blacklist
3. Don’t load blacklisted elements

Examples:

Ghostery, Disconnect, ShareMeNot, …



Blacklist Issues

- Require maintenance
  - Update and distribute the blacklist
- Any errors interfere with non-tracking services
  - Require fine-tuning
- Can be bypassed
  - Cannot handle third-party server tricks

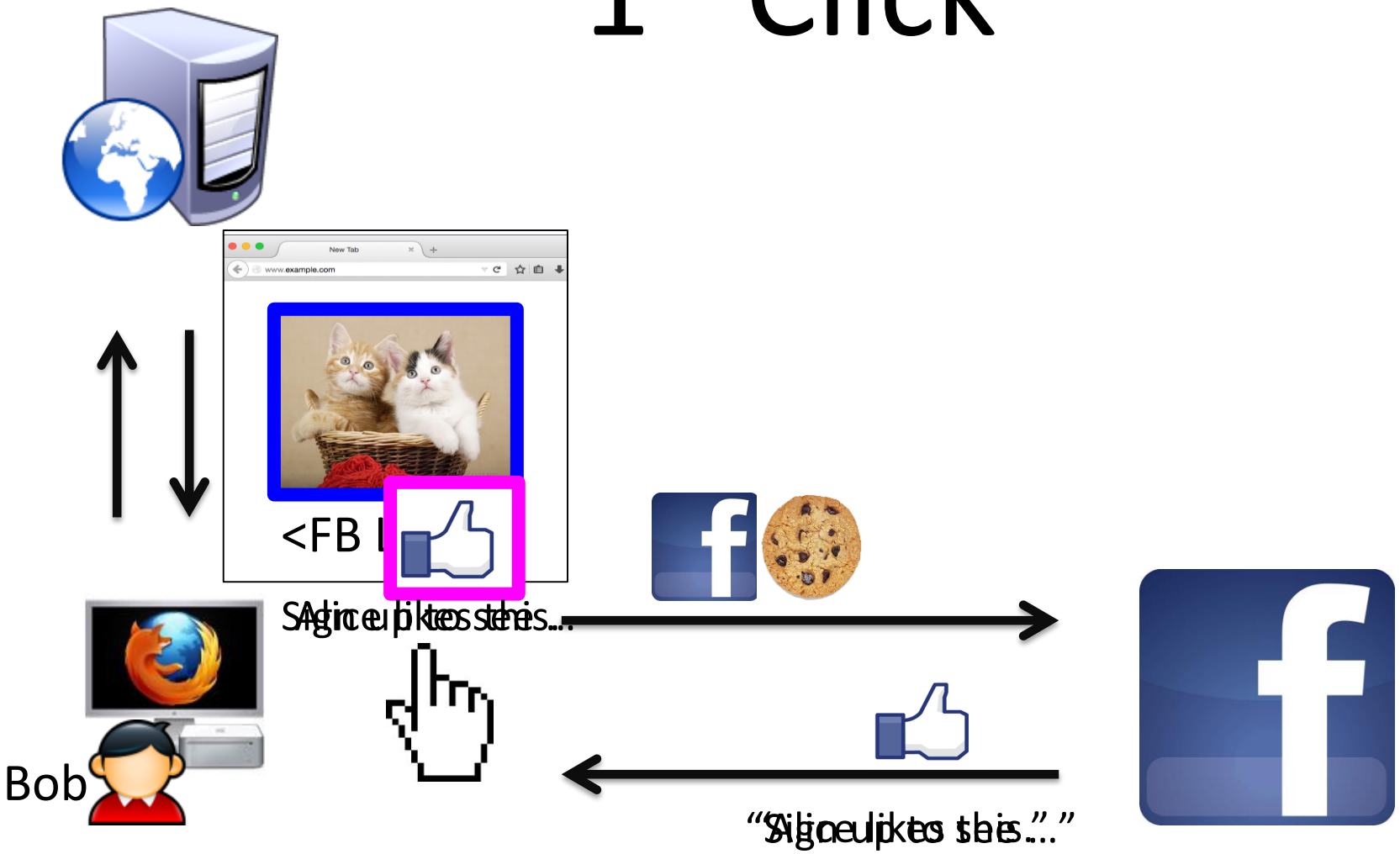
Our Approach

1. Load all third-party content without sending any cookies
   - **Allow whitelisting** desired third-party content
2. Reload third-party content with associated cookies if the user interacts with it
   1. **First click** to activate the third-party content
   2. **Second click** to register the action

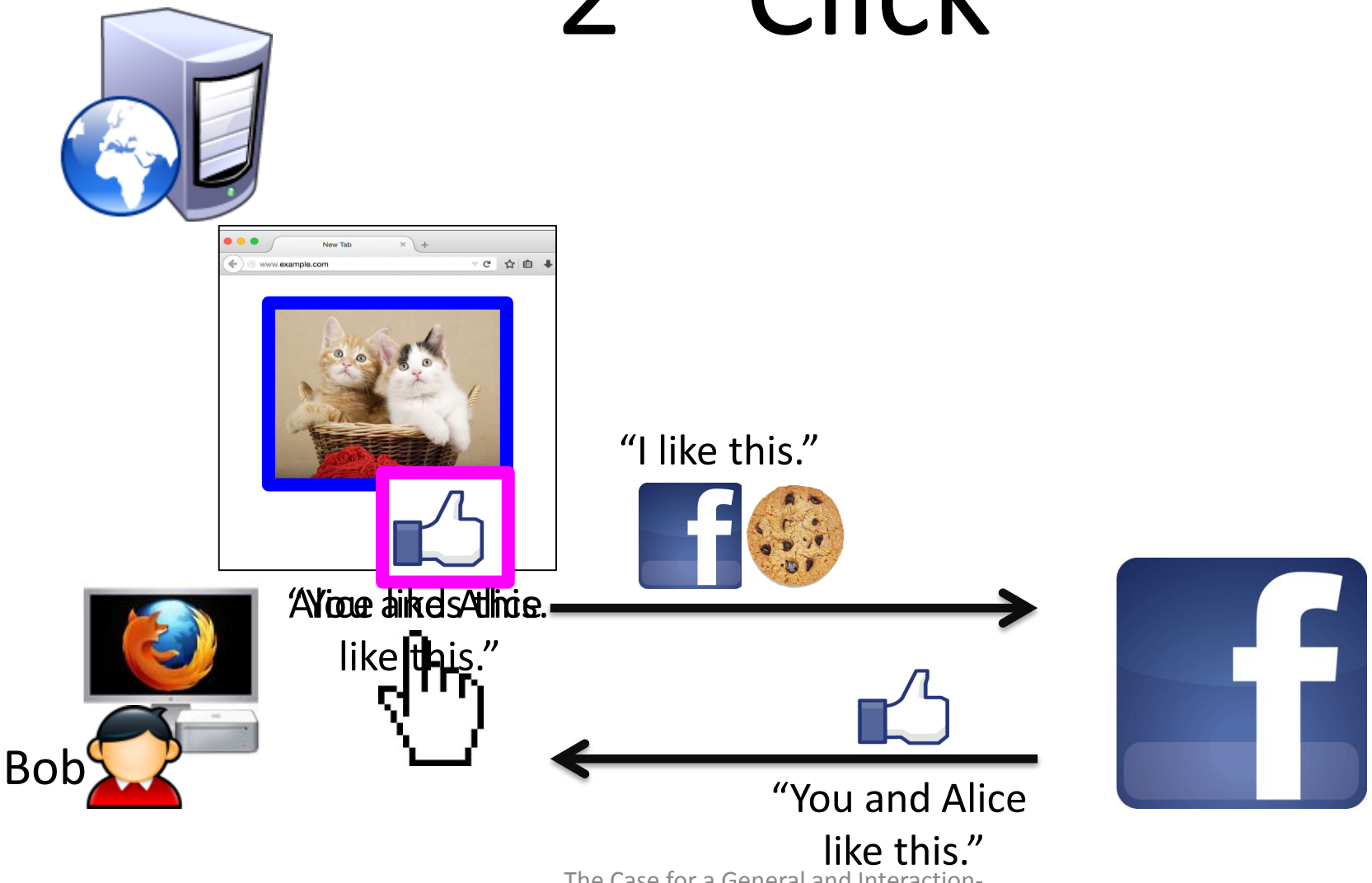
1. User interaction with two-clicks

2. Generalization with whitelisting

Interaction-based Policy: 1st Click



Interaction-based Policy: 2nd Click



Generalization

Bob

For any third party content!

User Interaction

All previous tools utilize it:

- Reload the entire page
  - Ghostery, Disconnect, ShareMeNot
- Selectively reload the interacted element
  - Priv3

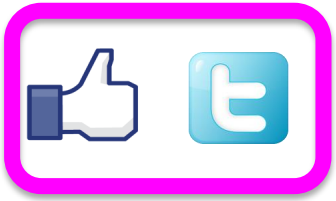
Still based on a blacklist!

1. We add the two-click control!

2. We generalize the concept!

Handling User Interaction

- Social widgets
  - Loaded in a single iframe; reload it



- Behavioral advertisements
  - Loaded in nested iframes; pass the click

➢ No interaction with ‘invisible items’
  - Small gif images, invisible iframes, …

Limitation of the Heuristic

- Advertisements loaded in a single iframe
  - Our policy will trigger a reload of the ad with potentially adverse side effects

- Future work: prevalence of this issue
  - Crawl the web and see how many ads are loaded in a single iframe

Outline

- Assumptions
- Existing approaches and shortcomings
- Our policy
- Discussion
  - Advertisement clicks
  - Lessons learned
- Implementation and preliminary evaluation
  - Priv3+
- Future & ongoing work

Advertisement Clicks

Why not also reload the advertisements?

- Nested iframes
  - Reload parent iframe?
  - Reload child iframe?
  - What if there is no source URL for the iframe?
- Click on the advertisement
  - "The user wanted to click **that** advertisement, not another."

Third-party Cookie Access

"Append-only" writing of visited sites

1. Third party script accesses its cookies on the user's browser
2. Adds pages visited to the cookies
3. Receives the cookies when the user visits it as a first party

➔Original Priv3 implementation prevents as does Priv3+

Lessons Learned

- General cookie policy: No blacklists
  - Unlike Ghostery, Disconnect, ShareMeNot, …
- More control for the user
  - On-demand social widgets requiring a little more user action (i.e., two-click control)
  - Whitelisting desired third parties
- No third-party tracking via cookies
  - No interference with non-tracking analytics and advertisement services
  - No tracking analytics and advertisement services

Priv3+

- Implemented for Firefox & Chrome
  - Emulates our general cookie policy in the browser
  - Two-click control for third-party content
  - Utilizes selective reload of interacted elements
  - Highlights various types of third-party content
  - Allows user to whitelist desired third-party content
- Downloaded over 14K times with ~3.1K active daily users

Preliminary Evaluation

- Top 1K popular sites from Quantcast, up to 10 pages
  - 7.3K pages
- Pageload time overhead compared with "accept all cookies"
  - Priv3+: ~4%
  - Never accept 3rd party cookies: ~1.7%
  - Accept 3rd party cookies from visited: ~1.3

Ongoing & Future Work

- Prevalence of single-iframe ads
- More comprehensive performance study
  - More sites, more pages
- Study of potential functionality issues
- User studies
  - Tracking expectations & treating of various 3rd party content

Summary

A general and interaction-based third-party cookie policy

- Prevents third-party tracking
- Enables social networking functionality on-demand
- Does not interfere with non-tracking services
- Implemented as browser extensions
  - Low overhead

Misc

- Evercookies
  - Flash cookies not deleted when clearing browser cookies
  - Revive cookie values by accessing flash cookies

➔ Cookies never received by third parties

- Cookie synching
  - Previous cookie values or first party cookies as GET parameters

➔ Previously set cookies will not be sent as to third parties and third party scripts cannot access cookies

Goal

Replicate the functionality of today's systems without tracking