From User Insights to Actionable Metrics
A User-Focused Evaluation of Privacy-Preserving Browser Extensions

Ritik Roongta
New York University (ritik.r@nyu.edu)

Rachel Greenstadt
New York University

Link to Paper

Introduction

- In 2023, average daily online time surpassed six hours, exposing users to more intrusive ad-tracking than ever before
- Privacy-preserving extensions (e.g., AdBlock Plus, uBlock Origin, Privacy Badger) reached 1B+ users but operate with extensive permissions that impact browser performance and site compatibility
- Despite their popularity, little is known about the nuanced user grievances these extensions provoke and how to quantify them.

Review Analysis

- We scrape Chrome webstore and collect 40k user reviews from different privacy-preserving extensions
- We filter 12.5k critical reviews using sentiment analysis and perform topic modelling on them to extract concers

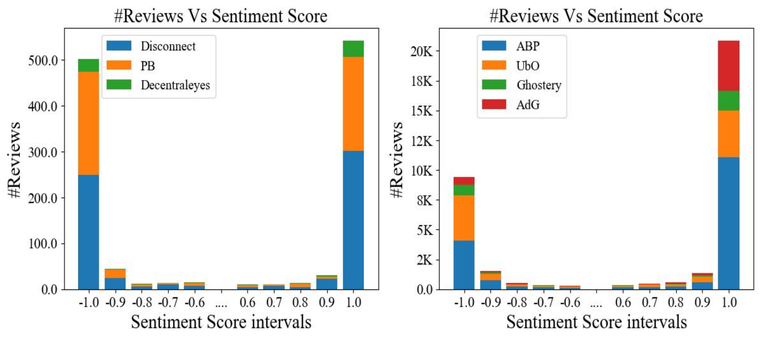


Figure 1: Critical Vs Non-Critical review sentiment score distribution

Topic Framework

- We applied topic modeling to the critical review dataset and uncovered 11 broad categories
- Each category is characterized by a curated set of related keywords that further define its themes

Broad Category	Related Keywords	#Reviews	Description
block	block, prevent, protect, secure, detect, bypass	4024 (32.01%)	Reviews that talk about blocking and detecting ads/malware, preventing websites from getting rendered, etc.
ads	popup, pop-up, malvertising, cdn, content delivery, spyware, adware, malware, paid, tabs, notification, annoy	911 (7.25%)	This category specifically covers pop-ups, spywares, CDNs, and other web objects that annoy people

Figure 2: Cropped snippet of the Topic Framework

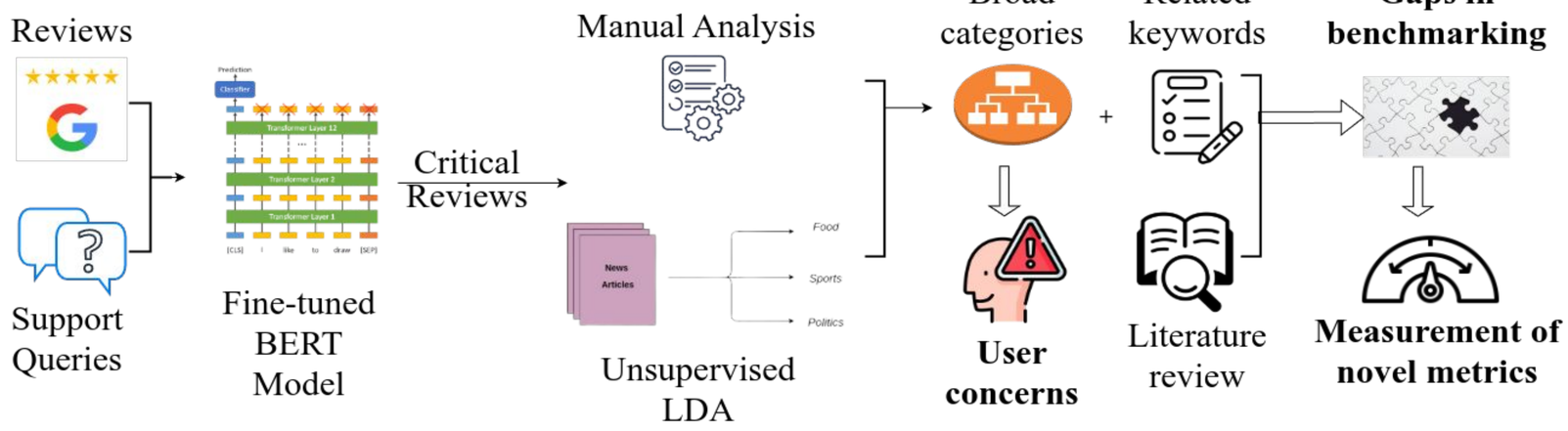


Figure 3: High-level architecture illustrating the extension analysis pipeline

User Concerns

We distill five user concerns from the review-based topic framework:

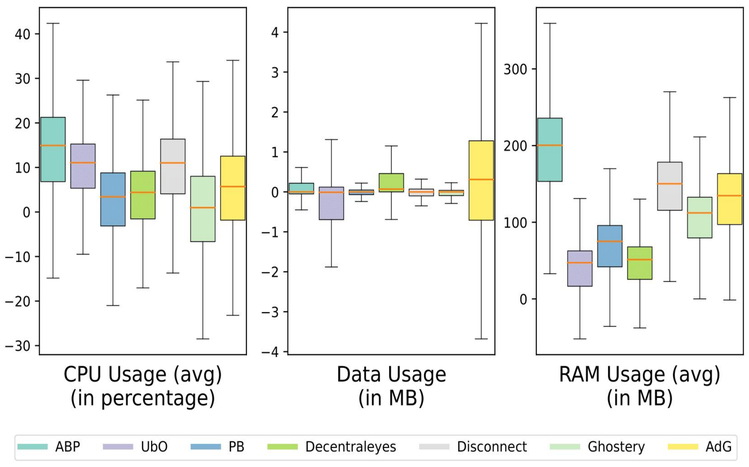
- **UC1 – Performance:** CPU load, RAM consumption, data overhead
- **UC2 – Web Compatibility:** "Disable ad-blocker" prompts, page hangs
- **UC3 – Data & Privacy Policy:** Permissions requested, storage use, policy clarity
- **UC4 – Extension Effectiveness:** Ads (frames) removed, third-party domains blocked
- **UC5 – Default Configurations:** Filterlist coverage, exception rules (e.g., Acceptable Ads)

Key Findings

- Past studies[1,2] measure extension performance but fail to include a variety of domains concerning users
- Different extensions perform well in different metrics we identify
  - **CPU usage:** Ghostery (best) vs. AdBlock Plus (worst)
  - **Data & RAM usage:** uBlock Origin has the best performance and AdBlock Plus has the worst
  - **Breakage prompts:** uBlock Origin & Ghostery least detected; AdBlock Plus most detected
  - **Permissions hygiene:** Ghostery requests the fewest unnecessary permissions; AdGuard the most
  - **Privacy policy compliance:** uBlock Origin & AdBlock Plus adhere closest to GDPR checks; Ghostery lags
  - **Ad blocking (frames):** Privacy Badger (PB) & Disconnect most effective; uBlock Origin least
  - **Tracker blocking (3rd-party):** uBlock Origin leading, followed by PB & Disconnect; AdBlock Plus least
  - **Filterlist configurations:** AdGuard and AdBlock Plus have a high number number of blocking rules but also rule exceptions. Other extensions have fewer blokcking rules

Examples

- The boxplot shows performance of different extensions on CPU Usage, Data Usage and RAM usage
- The dotted line represents the median
- Negative values signify better performance compared to the control case and vice-versa



Conclusion

- Our user-centered evaluation highlights that no single extension excels across all dimensions—trade-offs are inevitable
- By exposing 10 under-addressed metrics and piloting robust measurement techniques, we provide both researchers and developers with a clear roadmap for future benchmarking and improvement.

References

[1] Borgolte et al. Understanding the Performance Costs and Benefits of Privacy-focused Browser Extension (WWW 2021)
[2] Traverso et al. Benchmark and comparison of tracker-blockers (NTMAC 2017)