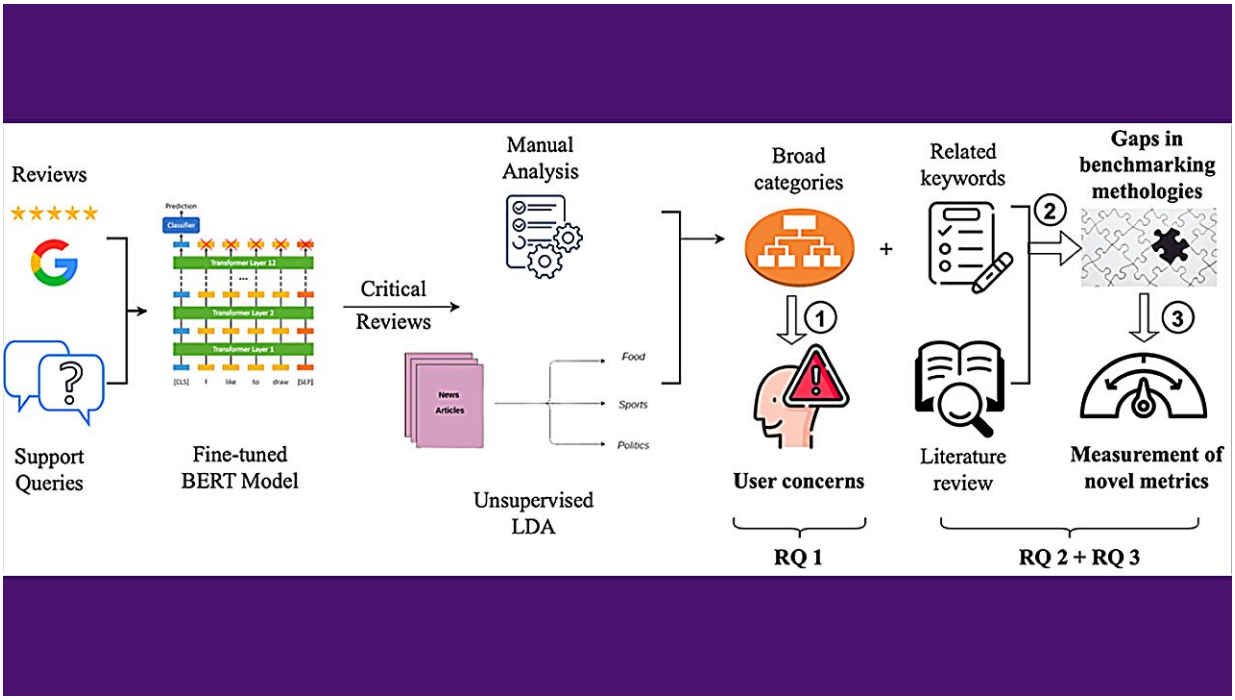
Privacy-enhancing browser extensions fail to meet user needs, new study finds

June 12 2024



The analysis unfolds in distinct stages as outlined in the flow diagram. Phase 1 involves developing the topic framework using review analysis, to identify user concerns (RQ 1). In phase 2 , through topic modeling and literature review, researchers find gaps in the benchmarking methods and introduce novel metrics for evaluation(RQ 2). Finally, phase 3 involves designing measurement experiments to evaluate the extension against the novel and existing metrics (RQ 3). The contributions are highlighted in bold. Credit: NYU Tandon School of Engineering

Popular web browser extensions designed to protect user privacy and block online ads are falling short, according to NYU Tandon School of Engineering researchers, who are proposing new measurement methodologies to better uncover and quantify these shortcomings.

Led by Rachel Greenstadt, professor in the NYU Tandon Computer Science and Engineering (CSE) Department, the team will present its study at the 19th ACM ASIA Conference on Computer and Communications Security, taking place July 1–5, 2024 in Singapore.

Through an analysis of over 40,000 user reviews of seven of the most popular privacy-preserving Chrome extensions, the researchers identified five key concerns among users: Performance, referring to the extent the extensions slowed down the system; Web compatibility, indicating how much they disrupted websites or caused substantial rendering delays; Data and Privacy Policy, pertaining to how the extensions handled user data; Effectiveness, evaluating how well they fulfilled their advertised purpose; and Default Configurations, assessing users' trust in the default settings.

"Our study found that there's a disconnect between what users want and what these extensions are actually providing," said Ritik Roongta, CSE Ph.D. student who is the lead author of the study. "Developers need to do a much better job of understanding and addressing the real-world pain points."

The researchers analyzed extensions that fall into two main groups. The first category, dubbed "Ad-Blockers & Privacy Protection," comprised extensions that block advertisements and third-party trackers. These include AdBlock Plus (ABP), uBlock Origin, Adguard, and Ghostery.

The second category, called "Privacy Protection," encompasses extensions primarily focused on enhancing user privacy by blocking

trackers and other privacy-invasive elements. This category includes Privacy Badger, Decentraleyes, and Disconnect.

The research team found that existing academic studies and benchmarking efforts had comprehensively explored just 4 out of the 14 key metrics underlying these five main user concerns. Crucial aspects like RAM usage overhead, ad-blocker detection likelihood, privacy policy soundness and adequacy of filtering rules were overlooked.

To bridge these research gaps, the researchers designed novel measurement methodologies and conducted extensive evaluation of the extensions against the unexplored metrics, providing a new benchmarking framework for evaluating the strengths and shortcomings of these privacy tools.

Their experiments involved smart crawlers visiting over 1,500 websites to analyze performance hits, compatibility issues, privacy policy strengths, ad-blocking capabilities and filter list configurations.

"The goal of this study is not to compare extensions specifically but to come up with a standardized benchmarking framework that addresses all user concerns so that the user can make informed decisions," said Roongta. "As extensions evolve with every update, they might over- or underperform in different metrics at different times."

The new measurement methodologies the researchers applied painted a mixed picture of the extensions they studied. While extensions like uBlock Origin optimized performance overheads well, most others like ABP exhibited significant CPU and memory overheads. Privacy Badger blocked ads and third-party trackers effectively while Ghostery struggled with them.

"Most of our analysis shows ABP needs to improve on metrics," said

Roongta. "That's because it whitelists certain ads to show to the users. While this new dimension is often perceived critically by the users, it is important to sustain a free Internet. It will be interesting to see how user preferences change as these standards evolve with the advertiser policies over time and the system gets better so that the overhead caused by the extensions is negligible."

The study highlighted instances of potential permission abuse and non-compliance with data protection regulations by some of the evaluated extensions. It provided recommendations for extension developers to enhance transparency around data practices.

The research underscores the pressing need for more rigorous analysis and systematic benchmarking of privacy-preserving browser additions that millions entrust with their online data and browsing experience daily. It contributes to Greenstadt's body of research that explores what happens when people try to use privacy-enhancing technologies and how the Internet responds.

More information: Roongta et al. From User Insights to Actionable Metrics: A User-Focused Evaluation of Privacy-Preserving Browser Extensions. (PDF)

Provided by NYU Tandon School of Engineering