Lane Gramling
EECS 700
Reading 12

# Summary - Adnostic: Privacy Preserving Targeted Advertising

This paper primarily focuses on whether the practice of online behavioral advertising can be done without sacrificing the privacy of the user. As the title suggests, the authors reimagine the architecture of an online behavioral advertising system with a proposal called Adnostic. Adnostic operates as a browser extension which focuses on relocating the data collection and behavioral profiling processes for a user into the browser, which keeps the user's behavioral profiling information from view and control by third parties.

## Contributions

Before diving into the design of their model, the authors first lay out the privacy and threat model which they are working around. Additionally, a section is dedicated to providing incentives for using Adnostic or a browser-based behavioral profiling structure in general, acknowledging that ad-networks need incentives to use this architecture otherwise there is no reason for them to change.

This leads the authors to the first major contribution of the paper, which is an elaborated outline of how browser-focused behavioral profiling would look and operate. Operation consists of processing behavioral information locally and keeping it contained within the user's browser profile where it cannot be accessed by third parties such as ad-networks, CDNs, and others. Adding to the paper's construction of this idea, the authors provide a reasonably convincing number of points arguing that there is in fact more incentive for both the user and the ad-networks to adopt this practice, including many points for behavioral profiles to have a far more accurate targeting system than their current models allow.

To supplement the primary contribution, the paper also contributes a number of different angles to this approach and embark on a valiant effort to test their argument against varying points of potential criticism. With this, the authors show how various portions of current ad-network models would remain unchanged, including click fraud detection, billing, ad serving, and potential attacks or other security issues.

## Limitations

While this amount of vetting is admirable, there are still a number of flaws visible with tier design. The proposed system for delivering ads over the network without showing the network what the user's interests are is highly inefficient, which relies on throwing a bunch of ads at the screen and 'seeing what sticks'. The authors attempt to address this, but their system for ad delivery still felt underdeveloped and like a potential pitfall if their argument was proposed to an ad-network. This could increase the cost of operating an ad-network significantly, and could easily outweigh the combined benefits of the incentives for ad-networks. Additionally, the system is not as anonymous as the authors claim, because even though ad clicks events must be sent to the ad-networks for click fraud detection mechanisms, this still shows the most powerful interests of the user to the ad-network and all other parties mentioned in their privacy model, therefore forcing this entire implementation to be used only to *reduce* the depth of information visible to these parties. Perhaps the argument would be better served with a suggestion of alternative means of click fraud detection and other accounting.

## Future Work

This paper suggests an idea with high potential in its utility for website developers, ad-networks, and end-users alike, but suffers from some fatal flaws which reflect directly in the cost of operation and considerably weaken the excitement built up the many legitimate incentives. As mentioned, their argument for browser-based behavioral profiling could be greatly strengthened with less regard for leaving current systems in place that they make sacrifices to accommadate (e.g. click fraud detection).