

An Evaluation of Self-Regulation of Consumer Tracking and Profiling: Deficiencies and Recommendations for Improvement

Submission to W3C Workshop on Web Tracking and User Privacy

28/29 April 2011, Princeton, NJ, USA

Keyna Chow, Nicholas Petersen & Chris Jay Hoofnagle

Samuelson Law, Technology & Public Policy Clinic

March 24, 2011

I. Introduction

This position paper is written on behalf of The World Privacy Forum (“WPF”) by members of the Samuelson Law, Technology & Public Policy Clinic at University of California, Berkeley School of Law. The WPF is a nonprofit, non-partisan 501(c)(3) public interest research group that works both nationally and internationally. The organization is focused on conducting in-depth research, analysis, and consumer education in the area of privacy.

Our project¹ evaluates self-regulatory principles² for online advertising, highlights their critical failings, and recommends alterations to the codes that better suit consumer privacy interests. Understanding these codes is critical for technologists, because technological approaches to web tracking and user privacy will be complemented by a mixture of self-regulatory norms and enforcement by the Federal Trade Commission (“FTC”).

At the April workshop, (1) we will explain how the policy debate on industry self-regulatory programs for online advertising is relevant to technologists, and (2) we will explore with the workshop participants whether flaws in self-regulation are purely policy issues or whether there are technical solutions to these challenges. Our presentation will emphasize:

- Political framing of the phrase “Online Behavioral Advertising” – does the phrase “Online Behavioral Advertising” (“OBA”) adequately address privacy concerns? Does that phrase accurately describe what is happening in a technical sense?
- Flaws and loopholes in the Network Advertising Initiative (NAI) and Digital Advertising Alliance (DAA) programs – can technology fill their policy gaps or do we need to strengthen the policy itself?

¹ On behalf of the World Privacy Forum, our project will produce a white paper evaluating the various self-regulatory programs for online behavioral advertising in May 2011. In addition, we submitted a comment to the Senate Commerce Committee discussing the key changes with the new NAI (*The NAI Then And Now: What Has Changed In Advertising Self-Regulation*, February 16, 2011) and a comment to European Advertising Standards Alliance (EASA) on its Best Practice Recommendations on Online Behavioral Advertising (*Comments on EASA Best Practice Recommendation on Online Behavioural Advertising*, February 25, 2011).

² We will evaluate, at a minimum, the NAI and the DAA principles in our project.

II. Background on Self-Regulation of Online Advertising

Our prognosis for the self-regulatory endeavor is bleak. Even at the most surface level, self-regulatory proposals fail to fully embrace the consumer privacy interests at stake.³ For example, the DAA's Self-Regulatory Principles for Online Behavioral Advertising does not even invoke "privacy" as a policy goal. It only refers to privacy descriptively (e.g. to identify "privacy policies" and the like), and does not recognize consumer privacy as a legitimate interest until page 35, where Internet service providers engage in Deep Packet Inspection.⁴

Without privacy as a policy goal, substantive provisions fail to address the most pressing issues at hand. Take, for example, Network Advertising Initiative's ("NAI") definition of the practice of online behavioral advertising: "OBA means any process used whereby data are collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments *for use in advertising online.*"⁵ This means NAI participants could be compliant, collect consumer data, and use that data for other purposes, so long as it is not for advertising online.

More broadly, tracking and profiling implicate consumer privacy whether or not data are used for advertising online. For the consumer, this means that opt-out abilities are largely illusory, because it only restrains *use* (not collection) of information for advertising purposes. The Principles sabotage the objectives that motivated intervention to begin with, dodge consumer concerns, and they thereby undermine the credibility of the self-regulation program. This and other self-regulatory codes stand upon a flawed foundation, and their regulatory codes reflect those foundational flaws.

III. Analysis

A credible self-regulatory scheme should meet certain minimum standards of independence, accountability, and structural features to maintain legitimacy. Our project explores what makes a good self-regulatory program and how well the various codes meet those expectations. We would like to present this research at the April workshop. Our preliminary research has shown that the self-regulatory codes submitted by the advertising industry are flawed and have ample room for improvement with regard to independence, accountability, and other self-regulation best practices.

³ National Consumer Council, *Models of self-regulation: An overview of models in business and the professions* 23 (November 2000), available at http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf ("The objectives must be rooted in the reasons for intervention"; "The scheme must be based on clear and intelligible statements of principle and measurable standards – usually in a Code – which address real consumer concerns." (emphasis added)).

⁴ Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising*, July 2009, <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>.

⁵ 2008 NAI Principles: *The Network Advertising Initiative's Self-Regulatory Code of Conduct*, pg 4, emphasis added, http://www.networkadvertising.org/networks/2008_NAI_Principles_final_for_Website.pdf

Independent scrutiny of advertisers is necessary to ensure consumer privacy is adequately protected.⁶ The proposed self-regulatory codes are not designed to protect privacy interests in a way that counteracts the financial incentives of online behavioral advertising. They lack the ability to critique their members unencumbered by their reliance on those members' financial support. Furthermore, the program does not command a sufficient share of the advertising market to make membership a prerequisite to doing business. The self-regulatory codes must take steps to expand membership so that they can overcome their financial reliance on the industry.

Embedded in the industry self-regulatory programs is a binary approach to privacy that can leave the consumer completely unprotected based upon choice or consent. For instance, the programs call for explicit consent to the adoption of technologies such as browser toolbars. Nothing in the programs calls for these technologies to be cabined through privacy-by-design approaches. Thus, once explicit consent is gained, the consumer can be tracked on all websites, even if there are approaches to limit the privacy impact of such a decision (such as anonymization, truncation of URLs, limits on data retention, limits on secondary use) while still giving the consumer the benefit of the technology. This all or nothing approach fails to protect consumers regardless of the choices they take.

The self-regulatory programs are also deficient with regard to their accountability programs. Their compliance reviews are inadequate, they fail to set clear thresholds for sanctions, and they provide inadequate statistical reporting requirements to allow the public to monitor compliance. This represents a missed opportunity, because enforcement can be used as a tool to benefit advertisers and consumers by giving consumers privacy protections in exchange for business goodwill that will follow trustworthy practices.

Other aspects of the self-regulatory programs that are too numerous to mention in this proposal lend themselves well to critique. Our project will explore the legitimacy of these programs by scrutinizing their terms, evaluating the extent they meet consumer needs, and suggesting how to revise them to improve their efficacy.

IV. Issues and Questions for Technologists

A. Does the name "Online Behavioral Advertising" adequately address policy concerns? Is it technically accurate to describe practices?

The name of the practice under discussion has been debated at least several times in its history. In 2000, the Federal Trade Commission ("FTC") referred to the practice as "Online Profiling."⁷ A 2009 FTC staff report now refers to the practice as "Online Behavioral

⁶ National Consumer Council, *Models of self-regulation: An overview of models in business and the professions* 23 (November 2000), available at

http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf ("As far as practicable, the operation and control of the scheme should be separate from the institutions of the industry").

⁷ "Online Profiling: A Report to Congress; Part 2: Recommendations," Federal Trade Commission, July 2000.

Advertising,”⁸ which is also the industry’s preference.⁹ The industry name for the practice is insufficient to embrace consumer concerns because it does not address the technological scope of the practice across multiple mediums¹⁰ or the temporal scope that embodies the life of the data through collection, use, and storage.

Our project refers to the practice under discussion as “Consumer Tracking and Profiling” because consumers’ interests should be preserved even after advertisers gain explicit consent to use consumer data. “Tracking and Profiling” embodies the meaningful control consumers require over their data after it is collected.

The industry automatically comes out ahead with the word “advertising” embedded in the phrase OBA because consumers are familiar with the concept of advertising and they value the services supported by advertising. However, this practice implicates privacy concerns beyond the traditional sense of advertising. Consumers may not know that seemingly anonymous data could be linked to their personal identities.¹¹ In addition, consumers’ data could be sold to another entity for purposes outside of advertising if the advertising network folds or merges in the absence of clear self-regulatory principles against doing so. For example, with the prominent use of online job applications, employers could in theory buy this data from advertising networks to screen candidates based on behavioral information.

The phrase OBA also does not indicate the level of knowledge consumers might have about what information advertisers have on them. Wiretapping or an early 20th century telephone party line may be a more apt comparison to understand this aspect of the practice. An advertising network may have picked up a receiver, so to speak, unbeknownst to the consumer browsing the Internet, who merely thinks he is communicating with the website owner. This advertising network does not only listen in to the conversation, but he may conference in others parties and record the conversation for his benefit.

“Consumer Tracking and Profiling” is just one proposal we have in an attempt to more accurately describe such practice. We welcome suggestions from technologists at the April conference for proposals on the framing of this practice.

⁸ “Self-Regulatory Principles For Online Behavioral Advertising,” Federal Trade Commission Staff Report, February 2009.

⁹ NAI 2008, pg. 4, available at:

http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf;

Self-Regulatory Principles for Online Behavioral Advertising, pg. 10, available at:

<http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>.

¹⁰ Including through applications that are not browsers, such as chat, and through other platforms, such as video game consoles.

¹¹ Testimony of Ashkan Soltani Before the Senate Committee on Commerce, Science, and Transportation Hearing on The State of Online Consumer Privacy, March 16, 2011 (“Despite some claims that these collected browsing profiles are “anonymous,” recent computer science research suggests that it is often quite easy to re-identify datasets that contain user information.”)

B. Even when users opt out, advertisers may still track them and deliver ads. How will this affect the public perception of the Do Not Track Header?

The self-regulatory principles under discussion limit a user's ability to opt-out. Consumers can only choose not to have their information exploited for online advertising. However, advertising networks could still collect data on all users, whether they opt-out of tracking or not. When a consumer opts-out, the data collected could be used for other purposes, so long as it is not behavioral advertising.

What do consumers expect to happen when they opt-out of the practice or alternatively, implement the Do Not Track Header on their browser? Do these self-regulatory principles undermine the expectation of no tracking from consumers? If the data collected is not used for behavioral advertising, what other purposes could they be used? Are those purposes necessary from a technical standpoint? Is there a way to technologically meet consumers' expectations on the collection of data?

C. Data retention is permitted by NAI and DAA principles "as long as necessary to fulfill a legitimate business need." How long do network operators really need the data?

The self-regulatory principles are extremely permissive in that they give businesses the ability to keep their data for essentially an unrestricted period of time. This is so because what constitutes a "legitimate business need" is left undefined. It is unclear how long businesses need to keep data to conduct behavioral advertising. How long is the data useful for the purposes of behavioral advertising? Are there diminishing returns, and are these quantifiable such they could inform a cost-benefit analysis?

D. The NAI employs four staff members, one of which monitors the compliance of its 66 members.¹² From a technical perspective, what would be required to monitor compliance? Is one person sufficient to fulfill this task?

Accountability measures should ensure that advertisers follow through on what they say they will do, e.g., stop behavioral advertising when a consumer opts out. Our white paper evaluates whether an appropriate amount of accountability exists in the self-regulation principles and will demonstrate that more can be done to ensure the integrity the programs. The question remains, however, what is entailed in evaluating compliance for dozens of advertising networks from a technical standpoint? Is one person enough to accomplish this task? What, in a technical sense, should accountability programs entail?

Conclusion

We look forward to discussing these issues with workshop participants and believe that there is a great opportunity for knowledge mobilization among technologists and lawyers in the challenge to meaningfully evaluate self-regulatory programs for online advertising.

¹² <http://www.networkadvertising.org/about/staff.asp>