
An Investigation of the Opt-Out State for Online Behavioral Advertising

Takahito Sakamoto

Intelligent Systems Laboratory,
Secom Co., Ltd.
Tokyo, Japan
takah-sakamoto@secom.co.jp

Naoki Watanabe

Intelligent Systems Laboratory,
Secom Co., Ltd.
Tokyo, Japan
watanabe-naoki@secom.co.jp

Masahiro Matsunaga

Intelligent Systems Laboratory,
Secom Co., Ltd.
Tokyo, Japan
m-matsunaga@secom.co.jp

Abstract

A recent trend in Internet advertising has been Online Behavioral Advertising (OBA). For users concerned about their privacy, advertising agencies provide users with an opportunity of user choice for OBA through the opt-out website. However, previous work shows that a lot of users misunderstand what it means to have opted out on the opt-out website. In fact, what actually happens when users opt out? In this study, we clarify the facts about being in the “opt-out state” for OBA, by crawling numerous websites and collecting browser cookies while opting out of OBA.

Author Keywords

Opt-out; online behavioral advertising; tracking; privacy; DAA; NAI;

Introduction

Online Behavioral Advertising (OBA) is based on web tracking and user profiling. Web tracking involves identifying a user device, browser, or app by using identifiers such as HTTP Cookie, and collecting user information through various websites the user visits. User profiling on the web is done to estimate a user’s attributes from many historical data collected by web tracking. OBA is known to be one of the most effective advertisement methods [4], but users are often concerned about its privacy implications for them.

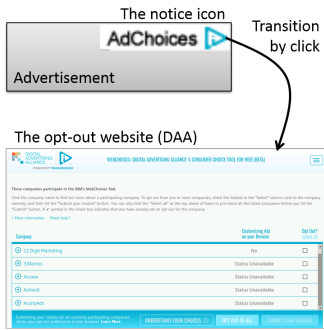


Figure 1: The opt-out icon and website.

Browser Cookie Storage

(a) Opt-out cookie
ad.example.com:
optout=1;

(b) Opt-out & ID cookie
ad.example.com:
optout=1;
uid=BEtYfxEZ7pJnDfmK
66fiY9Q7wprMRM7K;

The Federal Trade Commission (FTC) has published OBA principles [5, 7, 6], and associations of Internet advertising have published a guideline of self-regulatory principles for OBA [1].

As shown in Figure 1, an opt-out function was developed for transparency and consumer control based on this guideline: (i) the icon above a part of an advertisement provides consumers with a notice regarding online behavioral advertising; (ii) clicking the icon will take consumers to the opt-out website [2, 12] and provide an opportunity of user choice through the opt-out website. Then, the opt-out state for OBA is supposed to stop displaying advertisement based on user profiling, but not to stop collecting and profiling a user data.

According to McDonald and Cranor study [11], 34% of users expected that this opt-out turned off web tracking and user profiling as well. Furthermore, only 11% of users correctly understood the opt-out effect.

In this study, we investigate the opt-out state by analyzing browser cookies when users operate the opt-out function on the opt-out website. We identify two types of opt-out states. One state, which we call **E-optout** (Expected opt-out), aligns with users' expectations when opting out; namely, this state stops web tracking. The other state, **C-optout** (Compliant opt-out), minimally complies with the guideline that allows agencies to continue collecting user data after opt-out; namely, this state does not stop web tracking. We address the following research questions in this study.

- How many agencies are doing E-optout?
How about C-optout?
- How long is the opt-out state continuing?

Related work

Figure 1 shows the icon for the indicator used by Digital Advertising Alliance (DAA) and Network Advertising Initiative (NAI). When a user clicks this icon, a user can go to an opt-out website and control their opt-out state for several advertising third-parties. If a user enables the opt-out setting, an opt-out cookie related to a domain of an advertising agency is stored in their browser (left side bar (a)). After that, a user can indicate not to allow an OBA to the agency by sending the opt-out cookie when the user browses some websites.

Above that is an implementation of the opt-out function for OBA, though this opt-out is not for collecting and profiling user data, but just for receiving advertisement based on user information. In other words, the obligation of an agency is to stop collecting and profiling user data for OBA purpose, therefore an agency can continue web tracking and user profiling for other purposes. An advertising agency can set an identifiable cookie to the browser with an opt-out cookie (left side bar (b)), and still track a user.

McDonald and Cranor have already studied users on several usability for OBA [11]. Based on a survey of users' understanding of the opt-out effect on an opt-out website, their report shows that only 11% of users understood that opt-out is for advertising based on user information. In addition, 34% of users mistakenly believed that opt-out lets an agency stop collecting user data, and 18% of users believed that opt-out reduces the total number of ads shown to them.

Leon et al. [10] studied five individual opt-out websites as online survey. This report shows 57.9% of users incorrectly believe that the opt-out would stop both web tracking and tailored ads, only 13.4% correctly understood to stop tailored ads. Another Leon et al. report [9] also shows that no users correctly understood the opt-out meanings.

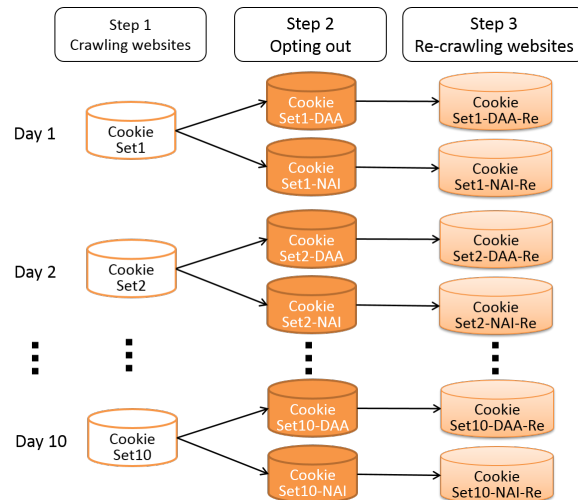


Figure 2: The method of investigation.

Komandori et al. [8] investigated the behavior of the opt-out cookies on the DAA and NAI opt-out websites. Their paper reported that most domains put an opt-out cookie into user browsers. However, their surveys did not investigate how many agencies continue web tracking with identifiable cookies after opt-out.

Methodology

We investigated many cookies by crawling three times per day for ten days. We conducted our observation over ten days from 10 July 2017 to 25 July 2017. In our observation we used OpenWPM [3] to crawl websites and collect cookies. The following explains each step.

Step 1: Crawling websites

Step 1 aims to collect cookies of advertising agencies that participate in DAA or NAI. We crawled the Alexa news category's top 100 sites for ten days in July 2017 while refreshing our cookie data each day.

Step 2: Opting out

We accessed the DAA and NAI opt-out websites and saved opt-out cookies while using a browser that had advertising cookies from Step 1. As shown in Figure 2, Step 2 generated separate cookie data for DAA and NAI from Step 1's cookie data.

Step 3: Re-crawling websites

We crawled the Alexa news category's top 100 sites again while using a browser with saved cookies from Step 2, and saved cookies after this crawling.

Analysis and findings

This section describes our method of analyzing the cookie data and the results of measuring E-optout and C-optout adoption.

The opt-out state which users expected

To classify into E-optout and C-optout, we first divided cookies into two sets based on whether they are identifiable to a browser or not. If a domain has identifiable cookies, an agency using the domain can track the browser. Below we give our definition of (non-)identifiable cookies.

- Non-identifiable cookie:
The cookie name and value are the same for all of days in a domain.
- Identifiable cookie:
Cookie values show some difference at least one for all of days in a domain.

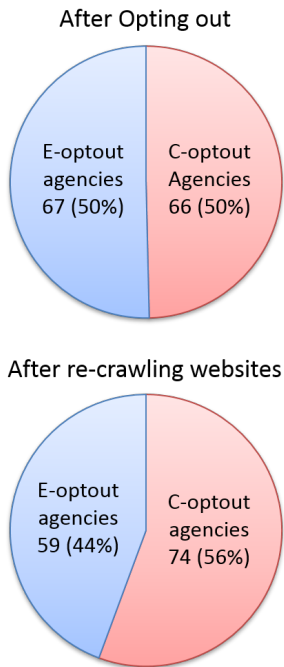


Figure 4: The results of E-optout and C-optout on 133 agencies.

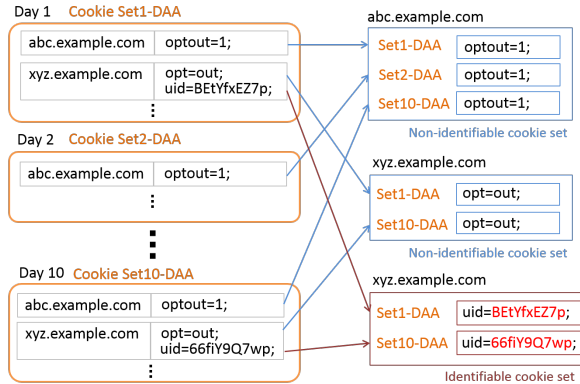


Figure 3: The classification method for non-identifiable cookie and identifiable cookie.

We used the cookie data collected in Step 2, and investigated 177 unique domains' cookies associated to 136 unique agencies, including both DAA and NAI. Here, we recognized that one agency had multiple domains, or multiple agencies used the same domain. However, we finally analyzed 133 agencies' cookies because we had not observed the cookies enough for three agencies.

Figure 3 shows our analysis method. We aggregated cookies for each domain across all days. For example, a domain "abc.example.com" has non-identifiable cookies because the cookie name and value are the same as "optout=1". Otherwise, a domain "xyz.example.com" has identifiable cookies because cookie values are different each day.

Figure 5 shows the aggregation method for E-optout and C-optout agencies. An E-optout domain is defined as the domain all has non-identifiable cookies. A C-optout domain is defined as a domain has at least one identifiable cookie.

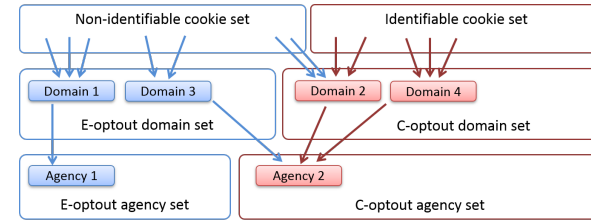


Figure 5: The aggregation method for E-optout and C-optout agency.

Furthermore, an E-optout agency is defined as an agency that only has E-optout domains. A C-optout agency is defined as an agency has a C-optout domain at least. We determined that around half of agencies stopped web tracking the same way as OBA after opting out on the opt-out websites.

Continuation of the opt-out

To investigate the continuation of the opt-out state, we analyzed Step 3's cookie data. As the result, 8 agencies started to track our browser again after Step 3. Finally, E-optout agencies comprised 44% and C-optout agencies comprised 56% of the 133 agencies studied, as shown in Figure 4.

Conclusion

In this study we investigated how many agencies implemented the opt-out that users actually expected for OBA opt-out. We found that around half of agencies stopped web tracking after opting out. However, some agencies started tracking again when users began browsing, so that 44% of agencies eventually stopped web tracking. As a result, we concluded that 44% of agencies met users' expectations. We believe that the more agencies meet users' expectations, the more usable OBA opt-out will become.

REFERENCES

1. AAAA, ANA, BBB, DMA, and iab. 2009. Self-Regulatory Principles for Online Behavioral Advertising. (2009). <http://www.iab.net/media/file/ven-principles-07-01-09.pdf>.
2. Digital Advertising Alliance (DAA). 2018. WebChoices: Digital Advertising Alliance's Consumer Choice Tool for Web (Beta). (2018). <http://optout.aboutads.info>.
3. Steven Englehardt and Arvind Narayanan. 2016. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of ACM CCS 2016*.
4. Ayman Farahat and Michael C Bailey. 2012. How effective is targeted advertising?. In *Proceedings of the 21st international conference on World Wide Web*. ACM, 111–120.
5. Federal Trade Commission. 2007. FTC Staff Proposes Online Behavioral Advertising Privacy Principles. (2007). <http://www.ftc.gov/news-events/press-releases/2007/12/ftc-staff-proposes-online-behavioral-advertising-privacy>.
6. Federal Trade Commission. 2009a. FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising. (2009). <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>.
7. Federal Trade Commission. 2009b. FTC Staff Revises Online Behavioral Advertising Principles. (2009). <http://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles>.
8. Saranga Komanduri, Richard Shay, Greg Norcie, and Blase Ur. 2011. Adchoices-compliance with online behavioral advertising notice and choice requirements. *ISJLP* 7 (2011), 603.
9. Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. 2012b. Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 589–598.
10. Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. 2012a. What do online behavioral advertising privacy disclosures communicate to users?. In *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*. ACM, 19–30.
11. Aleecia M McDonald and Lorrie Faith Cranor. 2010. Beliefs and behaviors: Internet users' understanding of behavioral advertising. In *Proceedings of the 2010 Research Conference on Communication, Information and Internet Policy*.
12. Network Advertising Initiative (NAI). 2018. NAI Consumer Opt Out (Beta). (2018). <http://optout.networkadvertising.org>.