
Cookie Confusion: Do Browser Interfaces Undermine Understanding?

Aleecia M. McDonald

PhD Candidate
Carnegie Mellon
5000 Forbes Avenue
Pittsburgh, PA 15213 USA
am40@andrew.cmu.edu

Abstract

We performed a series of in-depth qualitative interviews with 14 subjects recruited to discuss Internet advertising. Participants held a wide range of views ranging from enthusiasm about ads that inform them of new products, to resignation that ads are "a fact of life," to resentment of ads that they find "insulting." We discovered that many participants have a poor understanding of how Internet advertising works, do not understand cookies, and mistakenly believe there are legal protections barring companies from sharing information they collect online. We found that participants have substantial confusion about the results of the actions they take within their browsers, and do not understand the technology they work with now. The user interface for cookie management in popular browsers may be contributing to confusion.

Keywords

Behavioral advertising, Cookies, Mental Models, Privacy

ACM Classification Keywords

H.5.2 User Interfaces. K.4.1 Public Policy Issues—Privacy.

General Terms

Human Factors

Copyright is held by the author/owner(s).
CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.
ACM 978-1-60558-930-5/10/04.

Introduction

Behavioral advertising, also known as targeted advertising, is the practice of collecting data about an individual's online activities over time for use in selecting which advertisements to display. Ideally, behavioral advertising is more profitable for sellers, and consumers benefit by seeing interesting advertising. However, online privacy, re-identification of seemingly anonymous information [12] and the legality of some behavioral advertising business practices [4] remain at issue. The advertising industry [1] and their allies [14] favor continuing an "industry self-regulation" approach. The Federal Trade Commission conducted numerous workshops and released guidelines for self-regulation [7]. In contrast, there are legislative proposals at the federal [5] and state [4] level. Industry self-regulation assumes consumers make rational choices and are able to act in accordance with their privacy preferences. In this paper we present findings from a series of interviews about participants' mental models of online privacy, finding they do not understand how the most basic forms of behavioral advertising work, and that browser user interfaces may contribute to user confusion. We expect to conduct a follow-up survey to determine the prevalence of the views held by our interview participants in the larger population.

Background

Despite the scrutiny behavioral advertising has received, only a comparatively few studies examine how users interact with behavioral advertising and what they think of the experience. In 2008, TRUSTe commissioned a report on behavioral advertising, finding 57% of respondents are "not comfortable" with history-based behavioral advertising, "even when that information cannot be tied to their names or any other

personal information." [15] Several academic scholars have also investigated this area. Anton et al. studied privacy concerns in 2002 and again in 2008, and found that "individuals have become more concerned about personalization with regard to customized browsing experiences, monitored purchasing patterns, and targeted marketing and research" in 2008 [3]. Gomez et al. estimated that Google Analytics tracks at least 329,330 unique domains, and found confusion in privacy policies containing "conflicting statements that third-party sharing is not allowed but third-party tracking and affiliate sharing are" [8]. Most recently, Turow et al. conducted a representative sample of Americans and found 66% do not want behavioral advertising, with three quarters or more rejecting common behavioral advertising practices [16]. While the Turow work is valuable because it quantifies the percentage of Americans holding particular views, the standardized phone interview format meant they were unable to discover why people hold those views.

Behavioral advertising can use a variety of technologies, but we focus on cookies for three reasons. First, most large advertising companies use third-party cookies. Second, we found participants had never heard of anything more complicated; of seven common technologies, only cookies had name recognition. Third, cookies have been around, discussed, and studied across decades [2, 9]. If behavioral advertising is understood well enough to support decision making, it is likely to be via cookies.

Approach

We performed a series of in-depth qualitative interviews with 14 subjects who answered advertisements to participate in a university study

about Internet advertising. Subjects were not informed this study had to do with behavioral advertising privacy, but raised privacy concerns on their own, unprompted. We followed a modified mental models protocol of semi-structured interviews [11], using standard preliminary questions for all participants while also following up individually to gather participants' understanding of behavioral advertising.

Our study ran from September 28th through October 1, 2009 in Pittsburgh, PA. We recruited participants with a notice on a website that lists research opportunities. Participants were compensated \$10 for an hour of their time. Of our 14 subjects, 8 were male and 6 female. Half were age 21–29 and half were age 30–59. In addition to a small number of qualitative, open-ended interviews, we also plan to extend this work with large-scale online surveys. We will be able to understand more about the prevalence of our participants' privacy views, technical knowledge, and decision-making ability.

Results

Overall, we found low awareness of behavioral advertising. In its simplest form, behavioral advertising depends on third-party browser cookies, yet we found participants are not sure what cookies are or how they work. Most commonly, they confused cookies and history. Web browsers' user interfaces may contribute to users' mistaken mental models of cookies, which in turn makes it difficult for users to understand or make choices about behavioral advertising.

Impressions of Internet Advertising

We began all interviews by asking the open-ended question "What is Internet advertising?" The answer

given most immediately was "pop ups," with all but four participants mentioning pop ups. Banner ads are tied with pop ups for the most prevalent response. Banner ads were not usually mentioned first (as pop ups were) and were rarely mentioned by name. However, participants were quite capable of describing banner ads even without the vocabulary to name them. Five named "spam" as a form of Internet advertising.

Some participants gave characteristics of ads, rather than examples of ads. Six mentioned video and audio ads, usually while expressing displeasure at ads they find distracting. Participants also mentioned difficulty closing ads, and in particular complained that pop ups do not necessarily have a close button in the same place. The following concepts were mentioned by one participant each: viruses, hijacked links within articles, a constant stream of pop ups, and behavioral advertising (not mentioned by name, but described). The other thirteen respondents did not mention or allude to behavioral advertising at all when asked to define Internet advertising. Overall, the picture that emerges includes only a general familiarity with advertising, and some user frustration with specific advertising methods and modalities.

Four things were striking about these opening conversations. First, discussion of "relevant" ads ran the gamut from support to deep concerns about privacy. Second, participants were largely pragmatic about advertising. Even when they had scathing remarks about bad experiences, on the whole they understand and accept the model that advertising supports content. Their frustrations are generally not due to the existence of advertising, but rather to specific practices. Third, participants expressed anger

and frustration about advertising tactics they see, even when they do not understand the data being amassed about their online activities that they do not see. Finally, all of the issues raised above were volunteered, not prompted, after very open-ended questions at the start of the interviews. Participants' voiced concerns about advertising practices, behavioral targeting, and privacy in the first few minutes of discussion. Privacy is central to how participants perceive online advertising.

Misperception of Cookies

Because cookies are commonly used in behavioral advertising, we asked several questions regarding cookies. All participants had heard of cookies before. However, when asked, "What is a cookie?" four participants replied that they were not sure. Five participants gave an answer that was at least partially correct without also saying something factually incorrect. Only one person articulated that a cookie can contain a unique identifier.

Most people believed something that was not correct about cookies. Two people mistakenly believed that cookies store far more than they do, such as all actions they take online. Two people thought cookies regularly store personally identifiable or sensitive data like social security numbers, credit card numbers, and IP addresses. Two people described warnings for self-signed certificates and mistakenly believed that those warnings pertained to accepting or rejecting cookies. Three participants believed cookies are malware.

Only three of our fourteen participants said that cookies are related to personalized advertisement. They had three very different perspectives ranging from outright rejection, to seeing some benefits but finding harms

outweigh them, to support that is conditioned on the mistaken view that current practices are illegal.

Cookies Confused with Browser History

Participants did not understand that browser history is stored independently of cookies. Eight participants confused cookies with browser history, including one participant who believed the backward and forward arrows in a web browser depend on cookies. One participant told us cookies contain a "history of websites" visited and that if he deletes cookies, then "hyperlinks in different colors goes away, that's what it does. It clears the navigation history." He related how when he was a child living at home with his mother, he lost his computer privileges because she could see where he had been based on the color of web links, which he blamed on cookies. More exploration revealed that in his view, cookies were only an issue on computers where he shared a single account with multiple people as he had in his mother's home. At work, where he signed into his computer account with his own password, he believed cookies could not provide details of his browsing history because he was the only one with access to the account. Notice the confusion around password-protected accounts and privacy protections: several participants had confusion in similar areas.

Web Browser User Interfaces May Promote Confusion

Participants explained how they use web browsers to interact with cookies. One component of user confusion is temporal: participants reported they delete cookies and clear history at the same time, which leads them to misattribute properties of browser history to cookies. The reason participants clear cookies and history together likely stems from the way they are swirled

together in the user interfaces of web browsers. For example, Firefox presents choices about cookies, history, and bookmarks on the same tab. There is no visual hint that these three topics are distinct. To the contrary, cookies are in the middle of options for history, which serves to convey history and cookies are related. Moreover, Firefox does not expose any cookie options unless users know to change a setting on the Privacy Tab from “Remember history” to “Use custom settings for history.” Anyone looking through preference tabs for cookies will find no mention of them in the default configuration.

Unclear On Deleting Cookies

Nine of our 14 participants self-reported that they clear cookies. Only one of those nine said they clear cookies on their computer for privacy. Another three clear cookies only on shared machines. People told us they clear cookies for the following reasons:

- To delete history
- To avoid malware (viruses, spyware)
- To reduce clutter
- To save space
- Out of habit
- For “hygiene”

Participants have a vague notion that too many cookies are bad but do not know why. For all that they do not understand how cookies work, they do understand some of the benefits of cookies, such as not needing to log back in every time they visit a website. They are not sure under which conditions they should delete or retain cookies.

Discussion

Web browsers may strongly affect users’ ability to make choices about their privacy online. Browsers’ user interfaces may contribute to user confusion by mixing cookies, history, and bookmarks. Web browsers give no notice of or access to Flash cookies, which may explain why even technologically sophisticated users are unfamiliar with Flash cookies and how they can “respawn” deleted cookies [13]. As another example, Internet Explorer implements P3P support, but information about P3P is buried in the user interface, and a study of online trust markers found none of the participants were familiar with the P3P icon [10]. The Internet Explorer P3P implementation works well in that it does not require user intervention. Based on default settings, users do not accept any third-party cookie that does not have an associated P3P policy with an opt out. In this way browsers can provide an enforcement mechanism that may be stronger and faster to take effect than any regulations. However, as the early history of cookies themselves and the current example of Flash cookies and P3P amply demonstrate, just because browsers *can* provide user control does not mean they *will*. Cookies were introduced fifteen years ago, yet we observed most participants do not understand even first party cookies. We plan to conduct additional research with a larger sample size to understand how well these findings generalize to Internet users.

Citations

[1] AAAA, ANA, BBB, DMA, and IAB. “Self-Regulatory Program for Online Behavioral Advertising,” (2009). <http://www.iab.net/media/file/ven-principles-07-01-09.pdf>

- [2] Ackerman, M. S., Cranor, L. F., and Reagle, J. 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce* (November, 1999). <http://doi.acm.org/10.1145/336992.336995>.
- [3] Antón, A. I., Earp, J. B., and Young, J. D. "How Internet Users' Privacy Concerns Have Evolved Since 2002," North Carolina State University Computer Science Technical Report # TR-2009-16 Submitted to *IEEE Security & Privacy* (July 29, 2009). http://theprivacyplace.org/blog/wp-content/uploads/2009/07/tr_2009_16.pdf.
- [4] Arias, M. L. "Internet Law – Behavioral Advertising in the United States," Internet Business Law Services (June 30, 2009). http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2237.
- [5] Boortz, A. R. "New Federal Privacy Bill in the Works: Behavioral Advertising "Beneficial," But Must Be Done "Appropriately"" AdLaw By Request (August 12, 2009). <http://www.adlawbyrequest.com/2009/08/articles/legislation/new-federal-privacy-bill-in-the-works-behavioral-advertising-beneficial-but-must-be-done-appropriately/>.
- [6] Davis, W., Online Media Daily, "Judge Dismisses Case Against ISPs That Worked With Closed NebuAd," (October 12, 2009). http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=115259.
- [7] Federal Trade Commission Staff Report, "Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology" (February 2009). <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.
- [8] Gomez, J., Pinnick, T., and Soltani, A. "KnowPrivacy," UC Berkeley School of Information Report 2009-037, (October 10, 2009). <http://www.escholarship.org/uc/item/9ss1m46b>.
- [9] Ha, V., Inkpen, K., Al Shaar, F., and Hdeib, L. 2006. An examination of user perception and misconception of internet cookies. In *CHI '06 Extended Abstracts on Human Factors in Computing Systems* (April, 2006). <http://doi.acm.org/10.1145/1125451.1125615>.
- [10] Jenson, C., Potts, C., and Jenson, C. "Privacy practices of Internet users: Self-reports versus observed behavior," *International Journal of Human-Computer Studies*, Volume 63, Issues 1-2, (July 2005) Pages 203-227.
- [11] Morgan, M. Granger, Fischhoff, B., Bostrom, A., and Atman, C. J. *Risk Communication: A Mental Models Approach*. Cambridge University Press (2002).
- [12] Ohm, P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. ____ (forthcoming 2010). <http://ssrn.com/abstract=1450006>.
- [13] Soltani, A., Canty, S., Mayo, Q., Thomas, F., and Hoofnagle, C. "Flash Cookies and Privacy," (August 10, 2009). <http://ssrn.com/abstract=1446862>.
- [14] Szoka, B. M. and Thierer, A. D., Targeted Online Advertising: What's the Harm And Where Are We Heading? (February 13, 2009). Progress & Freedom Foundation Progress on Point Paper, Vol. 16, No. 2, February 2009. <http://ssrn.com/abstract=1348246>.
- [15] TRUSTe, "2008 Study: Consumer Attitudes About Behavioral Targeting," (March 28, 2008). http://danskprivacynet.files.wordpress.com/2009/02/truste2008_tns_bt_study_summary1.pdf.
- [16] Turow, J., King, J., Hoofnagle, C., Bleakley, A., Hennessy, M. "Americans Reject Tailored Advertising and Three Activities that Enable It," (September 29, 2009). <http://ssrn.com/abstract=147821>.