Third-party Cookie Policy

Albert H Chen
hselin@stanford.edu

Amy H Yen
htyen@stanford.edu

I. Introduction

While third-party cookies enable new web functionalities, it can also expose users' browsing history without users' awareness. A person's web history inevitably reveals personal information, which could be maliciously exploited for economical and/or psychological harm. Furthermore, users' obliviousness impedes the use of market force to regulate these third parties. To address this ecosystem deficiency, browsers should disable third-party cookies by default – requiring users to explicitly "opt-in".

II. How third-party cookies work and the associated economics

Third-party cookies enable modern web functionalities such as single-sign-on authentication [1], web analytics [2], targeted advertisements [3], and social sharing [4]. They work by allowing third parties[1] to store and retrieve data (cookies) on the browser [5] [6]. The data may include browsing pattern, identification information, transaction records, etc.

Figure 1 demonstrates the process.

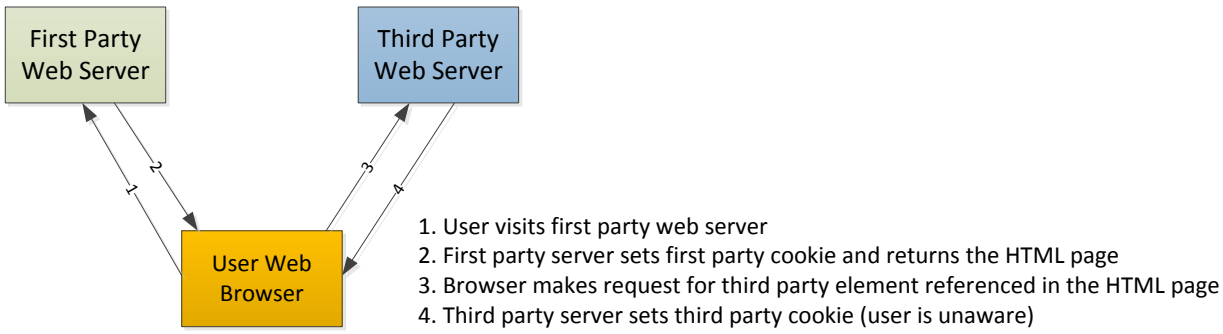

Figure 1: First and third party cookies

[1] Web sites not explicitly visited by the user

Figure 2 shows a visit to www.slate.com triggering many third parties behind the scene [7].

Figure 2: A list of third party tracking sites on http://www.slate.com

These third parties can then analyze or trade the collected information for economic gains. For example, Yahoo's ads network analyzes user history collected through first parties to display targeted ads [8].

III. Arguments for an "opt-in" policy

First, according to recent polls, the majority of online consumers are not willing to be tracked. According to a 2011 TRUSTe and Harris Interactive online survey [9], 78% of respondents would not consent to website analytics tracking, 85% would not consent to web browsing tracking for targeted ads, and 54% did not like online behavioral advertising. A 2013 TRUSTe survey [10] further showed that when options are available, 68% of respondents refused to allow their information to be shared with a third party and 52% would "opt-out" of online behavioral advertising. Thus, browsers should default to the majority preference.

Second, enabling third-party cookies by default could cause privacy and security concerns. The tracking information might be inadvertently leaked. For example, in 2010, Google reported a data leak caused by "human error" [11]. In 2011, hackers gained access to names and email addresses in Epsilon Data Management LLC's systems. This is a third party company managing marketing campaigns for first party firms. According to The Wall Street Journal, "in the days that followed, more than 40 companies—including J.P. Morgan Chase, TiVo and others—have said that their customers were among the victims" [12]. Regrettably, the victims are often oblivious to the involvement of third parties, and consequently do not know where to apply market pressure (such as boycotting) to force a more transparent and responsible data tracking.

Finally, there is a precedent for an “opt-in” policy. In 2009 the European Union passed the E-Privacy Directive legislation, which required websites to acquire visitor consent before installing cookies [13]. By adopting a similar policy, United States citizens will be afforded the same level of privacy and security protections enjoyed by the Europeans.

IV. Arguments against an “opt-out” policy

Proponents of an “opt-out” policy make several arguments. Each could be refuted.

First, the Interactive Advertising Bureau claims that an “opt-in” policy might break the advertisement support model of internet companies [14]. However, according to Jonathan Mayer [15], these effects could be mitigated with applications such as Adnostic [16] and Google Ads Preferences.

Second, proponents claim users could always “opt-out”. However, in practicality, the process is usually too difficult for average users. The opt-out option is often hidden and requires additional personal information [17]. According to a 2011 TRUSTe Research and Harris Interactive poll [9], only 37% of respondents consistently take steps to protect their personal information online while 26% do not know how to enable protection.

Third, proponents assert that tracking data would enable more personalized advertisements, which users prefer. However, surveys show that majority of users do not favor targeted ads. According to a 2010 USA Today/Gallup poll [18], 61% of respondents think the use of targeted ads to keep costs down is not justified, and 67% do not think targeted ads should be allowed. A 2012 survey by Pew Research [19] also found 68% of respondents dislike targeted ads because they do not want their online behavior tracked and analyzed.

Finally, proponents maintain that tracking data is anonymous. However, identity and tracking data could be correlated through various means. For example, first parties could sell their users’ identities to third parties, who could then associate their tracking data with these users’ identities [20] [21] [22].

V. Summary

Given the popular opinions and the harm that a security breach could cause, privacy should be the default rather than optional. I would strongly advocate that the United States government implement an “opt-in” policy, requiring browsers to disable third-party cookies by default.

References

[1] DISQUS, "Use of cookies," [Online]. Available: http://help.disqus.com/customer/portal/articles/466235-use-of-cookies.

[2] A. Kaushik, Web Analytics 2.0: The Art of Online Accountability and Science of Customer Centricity, John Wiley & Sons, 2009.

[3] Google, "DoubleClick cookies," [Online]. Available: https://support.google.com/adsense/answer/2839090?hl=en.

[4] engageclick, "Cookie Policy," [Online]. Available: http://engageclick.com/cookie-policy.html.

[5] Stanford University MS&E 233, "Privacy in a Networked World," 2013. [Online]. Available: http://www.stanford.edu/class/msande233/handouts/lecture12.pdf.

[6] D. Boneh, "Cookie Same Origin Policy," 2009. [Online]. Available: https://crypto.stanford.edu/cs142/lectures/10-cookie-security.pdf.

[7] Disconnect, "Disconnect | Online Privacy & Security," [Online]. Available: https://disconnect.me.

[8] The Wall Street Journal, "The Web's New Gold Mine: Your Secrets," 30 July 2010. [Online]. Available: http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404.

[9] TRUSTe Research and Harris Interactive, "Privacy and Online Behavioral Advertising," 25 July 2011. [Online]. Available: https://www.eff.org/files/TRUSTe-2011-Consumer-Behavioral-Advertising-Survey-Results.pdf.

[10] TRUSTe, "US 2013 Consumer Data Privacy Study — Advertising Edition," September 2013. [Online]. Available: http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=4NASFY29-418.

[11] PCWorld, "Google Blames 'human Error' for Data Leak," 12 Jan 2010. [Online]. Available: http://www.pcworld.com/article/186719/article.html.

[12] The Wall Street Journal, "Breach Brings Scrutiny Incident Sparks Concern Over Outsourcing of Email Marketing," 5 April 2011. [Online]. Available: http://online.wsj.com/news/articles/SB10001424052748704587004576245131531712342.

[13] European parliament and council, "DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," 25 November 2009. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.

[14] U.S. News & World Report, "'Do Not Track' Rules Would Put a Stop to the Internet As We Know It," 3 January 2011. [Online]. Available: http://www.usnews.com/opinion/articles/2011/01/03/do-not-track-rules-would-put-a-stop-to-the-internet-as-we-know-it.

[15] J. Mayer, "DO NOT TRACK IS NO THREAT TO AD-SUPPORTED BUSINESSES," 20 January 2011 . [Online]. Available: https://cyberlaw.stanford.edu/blog/2011/01/do-not-track-no-threat-ad-supported-businesses#DNT_ECONOMICS_FN2.

[16] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum and S. Barocas, "Adnostic: Privacy Preserving Targeted Advertising," in *NDSS*, 2010.

[17] MarketPlace, "How hard is it to opt out of third party data collection?," 22 May 2013. [Online]. Available: http://www.marketplace.org/topics/tech/how-hard-it-opt-out-third-party-data-collection.

[18] "USA TODAY/GALLUP POLL," December 2010. [Online]. Available: http://gallup.com/poll/File/145334/Internet_Ads_Dec_21_2010.pdf.

[19] Pew Research, "Search Engine Use 2012," 9 March 2012. [Online]. Available: http://www.pewinternet.org/2012/03/09/search-engine-use-2012/.

[20] A. Narayanan and V. Shmatikov, "Myths and Fallacies of 'Personally Identifiable Information'," *Communications of the ACM,* vol. 53, no. 6, pp. 24-26, 2010.

[21] J. . R. Mayer and J. C. Mitchell, "Third-Party Web Tracking: Policy and Technology," 13 March 2012. [Online]. Available: https://cyberlaw.stanford.edu/files/publication/files/trackingsurvey12.pdf.

[22] A. Narayanan, "THERE IS NO SUCH THING AS ANONYMOUS ONLINE TRACKING," 28 July 2011. [Online]. Available: https://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking.

This essay was reviewed by: Kevin Chaves (Humes Writing Center).
We did not review anyone's paper.