End the charade: Regulators must protect users' privacy by default

Christopher Soghoian
Center for Applied Cybersecurity Research, Indiana University
Draft of position paper for the Office of Privacy Commissioner of Canada

If you listen to executives from the online advertising industry, data aggregators, advertising supported webmail and social networking sites, consumers are extremely savvy. According to them, consumers know how to delete cookies,[1] and manage their browsers' privacy settings to protect themselves from data leakage via referrer headers, CSS history stealing attacks and super cookies; they read through hundreds of advertising network privacy policies, and opt out of just those ad networks and data aggregators whose policies disclose problematic practices; they are aware of the risks associated with insecure (HTTP) web browsing when using public WiFi networks, and thus seek out and enable poorly documented SSL options in the services they regularly use; and of course, they customize their social network privacy settings, and don't make any mistakes in the process.

This mythical tech-savvy consumer does not exist, even working within computer science departments, the offices of government privacy regulators, or the advertising firms themselves.

The vast majority of consumers do not understand cookies, have never heard of super cookies, referrer headers, or CSS history stealing, have likely never even tried to modify their browser' privacy settings, have never read a privacy policy (and likely think that the mere presence of a privacy policy means that the site does a good job in protecting their data), have never opted out of a behavioral advertising network (and probably couldn't name one, if asked), have no idea about the risks of checking their Facebook or Hotmail account at Starbucks, even after *Firesheep*.[2] Finally, if they have tried to customize their Facebook privacy settings, they probably made several mistakes in the process, and likely believe that their data is far better protected than it really is.

If the average consumer even knew about the numerous tools, browser add-ons and options to protect their privacy, many would be overwhelmed – however, most do not even know about these options, nor have they spent any time seeking them out, because they have no idea about most of the threats. When people think about privacy problems on Facebook – they think of their parents, ex-lover or employers seeing their private wall posts, not data brokers like Rapleaf building up dossiers to be sold for pennies to any interested buyer. Likewise, the only harm that most consumers reasonably expect at Starbucks is the obscene price of a *latte*, not the possibility that their email or social networking account can be hijacked by a hacker.

As one further data point, if executives at major websites like MSNBC, The Huffington Post, and Dictionary.com have no idea about the tracking cookies delivered via their own websites,[3] how can we reasonably expect consumers to understand the practice?

---

[1] http://econsultancy.com/us/blog/5257-study-flash-cookies-are-not-the-answer-for-online-advertising
[2] See generally: http://codebutler.github.com/firesheep/
[3] http://online.wsj.com/article/SB10001424052748703957804575602730678670278.html

It is time for government regulators to stop entertaining this charade of privacy policies that no one reads and opt-outs that no one uses. Consumers do not need to know how to change their oil to drive a car, and they should not need to know how to tweak obscure browser settings in order to safely browse the web. Regulators need to make sure that consumers receive comprehensive privacy protection, **by default**.

The key to doing this, I believe, is to transform the web browser into an effective privacy-enhancing technology. The web browser already controls the storage and transmission of cookies, supercookies and the transmission of referrer headers. Likewise, the browsers already include many configuration options and settings that, when correctly tweaked, significantly limit the degree to which consumers can be covertly tracked online.

Unfortunately, none of the browsers currently effectively protect privacy by default. One reason for this current state of affairs, at least for Chrome and Internet Explorer, is that these software products are created by online advertising networks, whose own profits would be hurt if users could not be tracked.

A Wall Street Journal exposé earlier this summer documented the internal deliberations over Internet Explorer's *InPrivate Filtering* feature, which, when enabled, blocks access to many third party servers, including behavioral advertising networks. As the Journal revealed, Microsoft's online advertising division was able to force the Internet Explorer team to disable this feature by default, and further require that users re-enable it each time the browser restarts. Because most users never change their software defaults, the effective impact of this decision was to expose millions of consumers to online tracking by behavioral advertising companies, including Microsoft's Atlas Solutions division, who would have otherwise have been protected had the feature been enabled by default.

Of course, Microsoft and Google could modify their web browsers to block all advertising networks other than their own. Such an action would prevent most forms of tracking, while still protecting the companies' respective profit margins (and perhaps even increasing them, as advertising dollars would likely shift to their own networks). However, it is likely that such an action would raise significant antitrust issues – and so we are left with the present situation, in which consumers are exposed to silent tracking by hundreds of different ad networks.

In order to ensure that consumers are protected from various forms of online tracking, privacy regulators should compel the major browser vendors to modify their products. At a minimum, I recommend the following:

- Third parties should not be permitted to track users across different sites and over multiple browsing sessions. The browser vendors should either block both the setting **and** transmission of 3rd party cookies and supercookies by default,[4] or should "double key" them

[4] "A further complication is that the three browsers referred above still transmit existing cookie information even when the browser settings are set to reject (new) 3d party cookies. In other words, information about cookies which have been placed before setting the browser to reject cookies will continue being sent to the ad network provider. Only one major browser currently allows users to both block the setting and the transmission of 3d party cookie data (i.e., including cookies placed before the setting of the browser to reject cookies). This has as consequence that also cookies that have been set as first-party (when visiting the single website of, for example, a search engine or a social networking site) can still be read by that site when the user visits a site that has partnered with that first website." See: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf at page 14.

to both the first and third party domains, such that they can no longer be used to track users across different first party sites.[5]

- Flash cookies, and Flash itself should no longer be given a free pass. Regulators should hold Adobe accountable for the poor privacy default of its widely used browser plugin. Third party sites should not be able to set any Flash cookies, and until Flash cookies can be controlled, examined and deleted by the browsers, all Flash cookies should expire after some reasonable period of time (as they currently last *forever*).
- Referrer headers should no longer transmit the full URL of the page last viewed when a user connects to a third party site. Website owners have no legal right to know the search terms that draw visitors to their websites, and it is time to protect consumers from a practice in which the search engines are willingly, and proactively engaged. Chopping off everything after the "/" from third party referrer headers would both eliminate the leakage of search engine queries, and the sharing of online social network identifiers that have recently lead to major news stories, and lawsuits by class action firms.
- The browser vendors must follow Chrome's lead, and embrace silent, auto-updates for security fixes.[6] Consumers should not have to click on an annoying dialog (which they have been trained to ignore) in order to receive protection from security threats. All of the browser vendors, and popular software plugins like Adobe's Flash and PDF Reader must embrace this model. Consumers cannot be protected from rogue advertising networks abusing browser privacy flaws unless they are running up to date software.[7]

The behavioral advertising industry depends upon widespread consumer ignorance of the very practices in which these companies are engaged: Tracking users around the web, building up detailed dossiers on their browsing activities and combining them with profiles purchased from data brokers. For too long, these companies have taken advantage of consumers' ignorance, and the sorry state of the privacy tools available to them. The best these firms have done is to offer up pathetic, poorly engineered opt-out mechanisms whenever the threat of regulation has appeared on the horizon, and embraced vague, loophole-riddled self regulatory frameworks that prohibit only the most heinous of practices.

Privacy by default will undoubtedly impact the advertising industry, and its ability to reach consumers. The industry has adapted to technical changes in the past, and it will certainly adjust to privacy-by-default. Regulators must put consumers' privacy first, and ensure that the tools that consumers use to browse the web are keeping them safe, rather than intentionally facilitating covert online tracking.

---

[5] See generally: https://wiki.mozilla.org/Thirdparty

[6] See: "Why Silent Updates Boost Security" Thomas Duebendorfer, Stefan Frei, ETH Tech Report, vol. TIK 302 (2009). http://www.techzoom.net/papers/browser_silent_updates_2009.pdf

[7] For an example of abuse of browser flaws by advertising companies, see: Dongseok Jang, Ranjit Jhala, Sorin Lerner, and Hovav Shacham. 2010. An empirical study of privacy-violating information flows in JavaScript web applications. In *Proceedings of the 17th ACM conference on Computer and communications security* (CCS '10). http://cseweb.ucsd.edu/~hovav/dist/history.pdf