August 2019

Cross-Site Tracking: Apple tightens its anti-tracking policies; Google proposes a long-term initiative

TOPICS: Cross-Site Tracking, Safari, Chrome, Privacy Sandbox, Google, Apple

Apple's Safari tightens its anti-tracking policies, including fingerprinting

Apple's Safari announced it will act to prevent all **covert tracking** and **cross-site tracking**, and **will treat websites and apps that attempt to bypass anti cross-site tracking features with the same seriousness as it does with regard to the exploitation of security vulnerabilities.**

The new policy, published by the web browser engine used by Safari, WebKit, states that web-tracking practices should be prevented by default as a matter of policy, as they are harmful to users and infringe on privacy rights.

This engine has implemented technical protections to prevent all tracking practices and **may expand the policy in response to other types of tracking without providing prior notice.** The policy focuses on access to privileged third parties, defined as a party that has the potential to track the user, across websites, without the user's knowledge or consent, due to the existence of special access built into the browser or operating system. According to this policy, such access to privileged third parties is not allowed, and merely hovering over, muting, pausing, or closing a given piece of content does not constitute a user's intention to interact with the party.

These restrictions may apply universally; to algorithmically classified targets; or to specific parties engaging in circumvention. **The engine will not grant any exemptions to the policy and, if faced with a tradeoff, will typically prioritize user benefits over preserving current website practices**. If limiting the capability of a technique is not possible without causing undue harm to the user, WebKit will request the user's **informed consent** to potential tracking.

Apple is not the first tech company to announce a crackdown on cross-site tracking, as its new policy was clearly inspired by **Mozilla's anti-tracking policy**.

Google presents a long-term initiative to enhance privacy on the web while minimizing harm to advertisers

Following Apple's move, Google announced its initiative to develop a set of open standards to enhance privacy on the web, **a long-term initiative referred to as "Privacy Sandbox".**

According to Google, although some other browsers have attempted to address this problem, without an agreed upon set of standards, those attempts are having unintended consequences, such as making it more difficult for online marketers and advertisers to obtain funding. **For Google, this jeopardizes the future of the web, as recent studies have demonstrated that when advertising is made less relevant by removing tracking, funding for publishers falls by an average of 52%.**

Google has shared preliminary ideas for a Privacy Sandbox - a secure environment for personalization that also protects user privacy. Some ideas include new approaches to ensure that ads continue to be relevant for users, but that user data which is shared with websites and advertisers, would be minimized by anonymously aggregating user information, and retaining far more user information on-device only. **This premise is built upon techniques such as Differential Privacy and Federated Learning.**

This long-term initiative is part of Google's Project Strobe, a project to analyze third-party developer access in its various services as well as Android's and Google's philosophy concerning apps' data access. One of the project's recent initiatives, includes Google requirement for third-party extension developers to be crystal-clear as to what information they want from users, and how they intend to safeguard that data and request access to the least amount of data. More extensions are required to post privacy policies, including extensions that handle personal communications and user-provided content. Developers that do not comply will be removed from the web store. **In our previous newsletter, we also reported on Google's plan to update Chrome in order to provide users with more transparency as to how sites are using cookies, as well as simpler controls for cross-site cookies.**

As we have been pointing out in our previous newsletters, the topic of cookies and other tracking mechanisms is regarded as being highly important as well as attracting widespread interest and should continue to be one of the most discussed topics in privacy this year. **On this matter, be sure to check our special Practical Cookie Consent Handbook.**

This update was published as part of our Technology & Regulation monthly client update. To read more about HFN's Technology & Regulation Department, **click here.**

Technology & Regulation Industry Spotlight

HERZOG FOX & NEEMAN
LAW OFFICE

Asia House, 4 Weizmann St., Tel-Aviv 6423904, Israel I Tel: (972)-3-692-2020 I Fax: (972)-3-696-6464
I hfn@hfn.co.il I www.hfn.co.il