

FTC Workshop on Cross-Device Tracking

Overview

The more advertisers know about their audience the better they can target them and the more publishers can charge for ad placement. When an individual uses multiple devices it prevents cookies from capturing a complete picture of the individual's browsing habits. According to an [AdExchanger article](#), "The more devices we have, the more fragmented our audiences and their cookies become." Cross-device tracking provides advertisers with a consolidated view of a person's interest. While this can improve ad revenues and product sales it is done at the cost of individual privacy.

Benefits of Cross-Device Connectivity

The ability to use multiple devices as one, provides individuals a seamless experience. When taken in isolation, services that provide individuals with cross-device connectivity help improve productivity and lower the frustration that can be caused by trying to use a single service across multiple devices. The effectiveness of having consistent browser bookmarks, password management and document editing tools across devices is a no brainer. Netflix has a great feature that lets consumers stream movies across multiple devices simultaneously. The ability to associate multiple devices with a single user is not something that should be challenged.

Enabling Cross-Device Tracking

Multiple Internet-connected devices can easily be associated with a single individual when that person logs into the same service using the same ID on each device. For example, logging into the same social network on multiple devices alerts the social network that the same person is using each device. The service can use the same cookie value across each device to create a combined profile based on the member's browsing habits, searches, posts and contacts.

A third party can benefit from an individual's cross-device identity by entering into an agreement with the service that owns the identity to share the identity of the individual with the third party. This can be done by sending the individual's ID to the third party or storing a unique ID from the third party and sending it back to the third party whenever the individual logs in on any device. This provides the ability for a third party that has no relationship with an individual to create a profile and benefit financially from the person's behavior.

Third parties can have agreements with multiple first-party services giving them greater ability to re-identify individuals when they use any of the services on any device. I discuss this in more detail in [my article](#).

The Perils of Cross-Device Connectivity

Now that a third party has the ability to track users across devices it can stitch together data collected when an individual is using a desktop computer at work, using a laptop at home, using a tablet at a friend's house and everywhere a smartphone is used. When location is enabled a person's workplace, home, restaurant preferences and favorite places can be tracked. Geolocation services can be used to identify churches, medical facilities, adult boutiques or other sensitive locations.

Unbeknownst to the individual, her browsing habits at home could be used when searching for items at work or viewing ads at a friend's house; revealing wedding, travel or birth plans. Individuals could also suffer from [price discrimination](#) when purchasing products, buying insurance or applying for a loan.

Opting out of behavioral advertising is not a viable remedy as it does not stop online tracking, data collection, creation of profiles or usage of profile data for other purposes.

Suggested Remedies

When looking to mitigate the risks that come from cross-device tracking care should be taken not to interrupt the beneficial features that come out of the ability to identify an individual across devices. The following is a list of what I feel are practical limitations that can be placed on entities that are able to track individuals across multiple devices:

1. Don't enable third-party cross-device tracking without explicit, informed consent.
2. Don't create profiles from behavioral data collected from multiple devices without consent.
3. Disable cross-device tracking and profiling when user is in "private browse" mode.
4. Provide transparency when syncing features enable tracking or cross-device profiling.
5. Permit users to limit tracking by device.
6. Permit users to see their data segregated by device with the ability to delete it.