Luxury Daily®

The News and Intelligence You Need on Luxury

COLUMNS

Problems with cookie tracking on Apple iOS

March 20, 2012

By Peter Hamilton

Picture a perfectly optimized mobile application campaign. Your graphics team designed an attention-grabbing image. Carefully crafted words evoke the proper buying emotion. Click-through rates are through the roof. The install rate is double the industry average.

Now picture the first experience a user has when she opens your app. After tapping the app icon on her iPhone, the user sees your app launch briefly. Then Mobile Safari launches and loads a blank page. Eventually Safari returns the user back to your newly installed app.

This technique is affectionately referred to as, "the switch." The goal is to get around cookie tracking limitations in iOS. It is also a lousy first impression for new app users.

Why is Mobile Safari loading a page?
App sandboxing prevents data sharing across iOS apps. Among other things, this means your app cannot read the cookie data stored by Mobile Safari.

To get around this, some tracking methodologies are opening Mobile Safari to search stored cookies for a matching key to associate with a newly installed app. This allows the tracking software to attribute an install to a previous event, such as viewing an ad on a

mobile site.

Because the app install has no way of knowing whether it originated via an organic install or an ad-initiated install, this cookie check happens on every app install. The result is the user seeing a visible switch to Mobile Safari and back.

How does iOS cookie tracking work?
The typical process where cookie tracking is used follows fairly consistent steps. The user visits a mobile site in Mobile Safari, views an advertisement, and a cookie is set.

If the user interacts with the ad, the cookie may also log the interaction event. When the user follows the advertisement call to action, she ends up on the App Store download page for the promoted app.

This is where cookie tracking temporarily loses visibility. The iTunes App Store passes no data about the install transaction.

As a workaround, some apps include tracking code that launches Mobile Safari to read cookie data that gets compared to an event ID and either do a URL GET to send data to an external tracking engine or do an HTTP POST to log the tracking information.

Once the cookie data is tracked, Mobile Safari relaunches the original app using a URL Schema.

Aside from the obvious flaw in forcing the user to open Mobile Safari, this process also leaves an open browser window with the tracking URL behind as a reminder.

If the user is on a slower connection, the entire tracking process can take as long as a minute, which is an eternity for someone who was excited to use your app for the first time.

Cookie tracking is fallible
In addition to being an ugly experience for your newly acquired user, cookie tracking is also fairly fallible.

If a user clears her cookies, any tracking data is lost and the install will be seen as an organic event.

Some cookie-based tracking solutions are attempting to get around cookie clearing by using the HTML5 local storage, but even the HTML5 cache may be cleared by the user.

On top of that there is the longevity of cookie tracking with the increasing popularity of ad blockers.

Is iOS cookie tracking the only way to track install?
Cookie tracking is not the only way to track app installs.

To attribute credit in app to app promotion, many ad networks and publishers use Device ID or Mac Address. These unique identifiers can be collected when a user clicks an advertisement in one app and when the user installs the promoted app.

However, Apple has already warned that it is taking away the use of Device ID, and I can only imagine that Mac Address will follow soon after.

The only trouble with Device ID and Mac Address is that you cannot collect these identifiers from the mobile Web. This is why mobile app marketers are turning to somewhat broader technology such as creating a user "fingerprint" by correlating many pieces of anonymous information from a user's device.

Developing a user fingerprint on the mobile Web is much different than on desktop.

Obviously the information you are able to collect from device is different, but you also have the challenge of matching these criteria to information that can be pulled through the mobile app on install.

These "cookieless" methods of tracking avoid the strange user experience of an added Safari pop up and visible redirect.

Don't forget the user

As marketers we invest a great deal of time and money creating an inviting experience for potential customers and clients.

We optimize landing pages with the ideal placement of images. Words are carefully chosen to evoke buying emotions.

It stands to reason we should also make sure the user has a great first experience once the app is installed.

By using tracking solutions that are transparent to the user, we still get the data we need to make smart business decisions, while continuing to put the user first.

Peter Hamilton is partner and chief marketing officer of HasOffers and Mobile App Tracking, Seattle. Reach him at peter@hasoffers.com.