Al Shaw and Jonathan Stray write: Twitter's mobile advertising arm enables its clients to use a hidden, undeletable tracking number created by Verizon to track user behavior on smartphones and tablets.
Does Your Phone Company Track You?
Check for Tracking Code

Click from your smartphone or tablet (with Wi-Fi turned off) to see if your telecom provider is adding a tracking number. We don't save any information.

Wired and Forbes reported earlier this week that the two largest cellphone carriers in the United States, Verizon and AT&T, are adding the tracking number to their subscribers' Internet activity, even when users opt out.

The data can be used by any site – even those with no relationship to the telecoms -- to build a dossier about a person's behavior on mobile devices – including which apps they use, what sites they visit and for how long.

MoPub, acquired by Twitter in 2013, bills itself as the "world's largest mobile ad exchange." It uses Verizon's tag to track and target cellphone users for ads, according to instructions for software developers posted on its website.

Twitter declined to comment.

AT&T said that its actions are part of a test. Verizon says it doesn't sell information about the demographics of people who have opted out.

This controversial type of tracking, known in industry jargon as header enrichment, is the latest step in the mobile industry's quest to track users on their devices. Google has proposed a new standard for Internet services that, among other things, would prevent header enrichment.

People using apps on tablets and smartphones present a challenge for companies that want to track behavior so they can target ads. Unlike on desktop computers, where users tend to connect to sites using a single Web browser that can be easily tracked by "cookies," users on smartphones and tablets use many different apps that do not share information with each other.

For a while, ad trackers solved this problem by using a number that was build into each smartphone by Apple and Google. But under pressure from privacy critics, both companies took steps to secure these Device IDs, and began allowing their users to delete them, in the same way they could delete cookies in their desktop Web browser.

So the search for a better way to track mobile users continued. In 2010, two European telecom engineers proposed an Internet standard for telecom companies to track their users with a new kind of unique identifier. The proposal was eventually adopted as a standard by an industry group called the Open Mobile Alliance.

Telecoms began racing to find ways to use the new identifier. Telecom equipment makers such as Cisco and Juniper began offering systems that allow the identifiers to be injected into mobile traffic.

In the spring of 2012, AT&T applied for a patent for a method of inserting a "shortlived subscriber identifier" into Web traffic of its mobile subscribers and Verizon applied for a patent for inserting a "unique identification header" into its subscriber's traffic. The Verizon patent claims this header is specifically meant to "provide content that is targeted to a subscriber."

Inserting the identifiers requires the telecom carrier to modify the information that flows out of a user's phone. AT&T's patent acknowledges that it would be impossible to insert the identifier into web traffic if it were encrypted using HTTPS, but offers an easy solution – to instruct web servers to force phones to use an unencrypted connection.

In the fall of 2012, Verizon notified users that it would begin selling "aggregating customer data that has already been de-identified" -- such as Web-browsing history and location -- and offered users an opt-out. In 2013, AT&T launched its version -- a plan to offer "anonymous AT&T data" to allow advertiser to "deliver the most relevant messages to consumers." The company also updated its privacy policy to offer an opt-out.

AT&T's program eventually shut down. Company spokesman Mark Siegel said that AT&T is currently inserting the identifiers as part of a "test" for a possible future "relevant advertising" service. "We are considering such a program, and any program we would offer would maintain our fundamental commitment to customer privacy," he said. He added that the identifier changes every 24 hours.

It's not clear how much of a hurdle changing the identifier would present to a targeting company that was assembling a dossier of a user's behavior.

Meanwhile, Verizon's service – Precision Market Insights – has become popular among ad tracking companies that specialize in building profiles' of user behavior and creating customized ads for those users. Companies that buy the Verizon service can ask Verizon for additional information about the people whose unique identifiers they observe.

"What we're excited about is the carrier level ID, a higher-level recognition point that lets us track with certainty when a user, who is connected to a given carrier, moves from an app to a mobile Web landing page," an executive from an ad tracking company Run told an industry trade publication.

And in a promotional video for Verizon's service, ad executive Chris Smith at Turn, touted "the accuracy of the data," that the company receives from Verizon.

But advertisers who don't pay Verizon for additional information still receive the identifier. A Verizon spokeswoman said, "We do not provide any data related to the

[unique identifier] without customer consent and we change the [unique identifier] on a regular basis to prevent third parties from building profiles against it." She declined to say how often Verizon changes the identifier.

The use of carrier-level identifiers appears to be becoming standard. Vodafone, a British telecom, says it inserts a similar identifier into some mobile traffic. A Vodafone spokesman said "Header enrichment is not our default operation and we do not routinely share information with the websites our customers visit."

However, ProPublica found a handful of Vodafone identifiers in its logs of website visitors. That review also showed more than two thirds of AT&T and Verizon visitors to ProPublica's website contained mobile identifiers.

And there appears to be no way to opt out. Last week, security engineer Kenn White noticed an Ad Age news article about Verizon's mobile marketing program and set up a test server to see if he was being tracked. He had opted out years ago, but he noticed a strange identifier in the web traffic from his phone.

His tweets sparked a flurry of discussion of Verizon's actions on the Hacker News discussion board, and articles in the technology press.

Software engineer Dan Schmads, an AT&T user, also tried to opt out. He found that he needed to visit four different webpages to opt out, including one web page not even on AT&T's domain: http://205.234.28.93/mobileoptout/. But he continues to see the AT&T identifier in his mobile traffic.

AT&T's Siegel told ProPublica that he appreciated the feedback on the difficulty of opting out and that the company plans to streamline the process before launching its service.

"Before we do any new program, we'll give customers the opportunity to reset their mobile ID at any time," he said. "It would be like clearing cookies."

Google has proposed a new Internet protocol called SPDY that would prevent these types of header injections – much to the dismay of many telecom companies who are lobbying against it. In May, a Verizon executive made a presentation describing how Google's proposal could "limit value-add services that are based on access to header" information.