DO VERIZON AND AT&T'S SUPER COOKIES COUNT AS SESSON IDENTIFIERS?

Over the past weeks, we've been learning more and more about a supercookie that Verizon and AT&T have stuck in the phone browsing of users on their mobile network. In the case of Verizon, you can't opt out of sending the supercookie any time you browse using Verizon's network, and websites you visit will be able to use Verizon's supercookie to track you as well.

> Whatever the merits of Verizon's new business model, the technical design has two substantial shortcomings. First, the X-UIDH header functions as a temporary supercookie.3 Any website can easily track a user, regardless of cookie blocking and other privacy protections.4 No relationship with Verizon is required.
>
> Second, while Verizon offers privacy settings, they don't prevent *sending* the X-UIDH header.5 All they do, seemingly, is prevent Verizon from *selling* information about a user.

Unless you opt out, this cookie will also track your your geography and demography.

Kashmir Hill has been doing great work on it, including today's responses from the two phone companies about what they've been doing.

> How long have they been tagging their users this way?
>
> Verizon: Two years. Given how long Verizon has been doing it, Kasowic said she was "surprised" by the attention this week.
> AT&T: "A little while." AT&T is just

> “testing it” at this point.
>
> Why are they tagging customers this way?
>
> Verizon: To deliver ads, to authenticate users and allow them to avoid filling out forms, and for fraud prevention.
> AT&T: To deliver ads.
>
> Is there any privacy protection built in?
>
> Verizon: The code is “dynamic” and will change on a “regular basis” — at least once per week.
> AT&T: The code is dynamic and will change daily.
>
> [snip]
>
> Can they opt out of anything?
>
> Verizon: Customers can’t opt out of the header code being sent “because it’s used for multiple purposes,” says Kasowic. But they can opt out of it being used to show them relevant ads. “When it’s used for the advertising program, there’s a place where information is tied to the UIDH (Unique Identifier Header) — such as ‘Females in Alexandria, VA. between the ages of 25 and 50,” said Kasowic. “It’s just segments that other people wouldn’t understand. There’s no personal identification. If you opt out, there’s no information stored there.” But the tracking code remains.
> AT&T: Siegel says customers will be able to opt out of ad delivery and tracking.

Among all the other worries I have about this, I have my lingering worry: that the government will use the supercookie if and when USA Freedom Act passes. As a reminder, here’s how USAF defines “call detail record,” which is a key part of their ongoing daily production.

> (2) CALL DETAIL RECORD.—The term ‘call

> detail record'—
>
> (A) means session identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call; and
>
> (B) does not include—
>
> (i) the contents (as defined in section 2510(8) of title 18, United States Code) of any communication;
>
> (ii) the name, address, or financial information of a subscriber or customer; or
>
> (iii) cell site location information.

This definition uses language tied to phone calls, but with the limited exception of the CDR definition used for NSLs, there is a well-established tradition of using phone CDR language to get Internet records. And a cookie is the quintessential "session identifier." While Verizon's supercookies might provide access to things that might qualify as content — "any information concerning the substance, purport, or meaning of that communication" — it would not seem to necessitate this. Plus, the supercookie would provide generalized location without cell site location.

In other words, the Verizon supercookie would provide FBI and NSA a way to get rich information on the target and his online actions — including co-presence on sites that might include chat rooms (which would serve as your hops) — that they could then match up to the backside, tracking the cookie on across the web. Depending on what Verizon uses it to authenticate users for, it may give a lot more. (Note, too, that Sprint appears to be working on the equivalent of a burner phone application for

mobile devices based off cookies; this supercookie would seem to make that even easier.)

The Yahoo example – where the government moved from requesting emails and instant messages to requesting 9 things, potentially across all of Yahoo's business units in 5 months – is instructive. Even if they aren't already planning on using this (which I doubt, given that it has been out there for 2 years), they will use it. And nothing in the bill seems to prohibit it.

I'm not convinced this is the only answer to my question about what connection chaining does. But I think it is one of answer.

Update: Propublica reports that Twitter has adopted Verizon's UIDH for its own advertising purposes.

> 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.