FACEBOOK'S FLIP-FLOP: IS IT A LAW ENFORCEMENT THING?

Kash Hill has a fascinating story about a Facebook flip-flop over a story she reported yesterday.

It started when — as increasingly happens in her work — someone came to her with a scary problem. Facebook recommended he friend someone he had only just met for the first time at a meeting for parents of suicidal teens. In response, Facebook confirmed they do use co-location for such recommendations.

> Last week, I met a man who was concerned that Facebook has used his smartphone location to figure out people he might know. After he attended a gathering for suicidal teens, Facebook recommended one of the other parents there as a friend, even though they seemingly had nothing else in common but being in the same place at the same time. He asked me whether Facebook was using location to figure out if people knew each other.
>
> I was skeptical, because that seemed like such an egregious violation of privacy. On Friday, I emailed Facebook:
>
> > A Facebook user told me that he attended an event last week with people he'd never met before. The next morning, one of the people at the event came up as a suggested friend. They had no other ties beyond being in the same room the night before. Could their shared location have resulted in the suggestion?
>
> A spokesperson responded, saying that location is one of the signals for

> "People You May Know."

But then, as people started making a stink about this, Facebook reached out again and offered this oblique reversal.

> Thus I reported that "Facebook is using your phone's location to suggest new friends—which could be a privacy disaster." The story garnered lots of negative feedback, with people upset about Facebook using their location information this way without telling them.
>
> Then, on Monday night, the Facebook spokesperson reached out again, saying the company had dug into the matter and found that location *isn't* currently used. She sent an updated statement:
>
> > "We're not using location data, such as device location and location information you add to your profile, to suggest people you may know. We may show you people based on mutual friends, work and education information, networks you are part of, contacts you've imported and other factors."

One part of this comment is easy: Facebook is not using locations you mark for yourself (so if I said I was in Grand Rapids, they wouldn't use that to find new Grand Rapids friends for me). But it's not really clear what they mean by "device location." Determined by what? GPS? Cell tower? IP location? Wifi hotspot colocation?

Which got me thinking about the way that federal law enforcement (in both the criminal and FISA context, apparently) are obtaining location data from social media as a way to tie physical location to social media activity.

> [Magistrate Stephen Smith] explained he had had several hybrid pen/trap/2703(d) requests for location and other data targeting WhatsApp accounts. And he had one fugitive probation violation case where the government asked for the location data of those in contact with the fugitive's Snapchat account, based on the logic that he might be hiding out with one of the people who had interacted with him on Snapchat. The providers would basically be asked to to turn over the cell site location information they had obtained from the users' phone along with other metadata about those interactions. To be clear, this is not location data the app provider generates, it would be the location data the phone company generates, which the app accesses in the normal course of operation.

Doing so with Facebook would be particularly valuable, as you could target an event (say, a meeting of sovereign citizens) and find out who had attended the meeting to see whose location showed up there. The application would be even more useful with PRISM, because if you were targeting meetings overseas, you wouldn't need to worry about the law on location data.

In other words, I started wondering whether Facebook is using this application — and was perfectly willing to tell Hill about it — until the FBI or someone started complaining that people would figure out one of their favorite new law enforcement (and intelligence) methods.

Hill is still pressing Facebook for real answers (and noted that Facebook may be violating FTC rules if they are doing this, so expects answers from there if not from Facebook directly).

Still, I'm wondering if FBI is now telling our private spy companies they can't reveal the techniques law enforcement most likes to rely on.