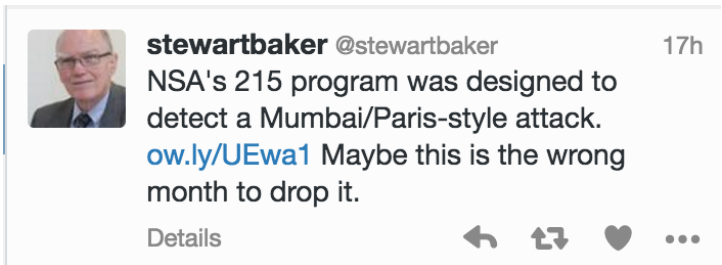
SURVEILLANCE HAWK STEWART BAKER CONFIRMS DRAGNET DIDN'T WORK AS DESIGNED

The French authorities are just a day into investigating the horrid events in Paris on Friday. We'll know, over time, who did this and how they pulled it off. For that reason, I'm of the mind to avoid any grand claims that surveillance failed to find the perpetrators (thus far, French authorities say they know one of the attackers, who is a French guy they had IDed as an extremist, but did not know of people identified by passports found at the Stade — though predictably those have now been confirmed to be fake [update: now authorities say the Syrian one is genuine, though it's not yet clear it belonged to the attacker], so authorities may turn out to know their real identity). In any case, Glenn Greenwald takes care of that here. I think it's possible the terrorists did manage to avoid detection via countersurveillance — though the key ways they might have done so were available and known before Edward Snowden's leaks (as Glenn points out).

But there is one claim by a surveillance hawk that deserves a response. That's former DHS and NSA official Stewart Baker's claim that because of this attack we shouldn't stop the bulk collection of US persons' phone metadata.



The problem with this claim is that the NSA has a far more extensive dragnet covering the Middle

East and Europe than it does on Americans. It can and does bulk collect metadata overseas without the restrictions that existed for the Section 215 dragnet. In addition to the metadata of phone calls and Internet communications, it can collect GPS location, financial information, and other metadata scraped from the content of communications.

The dragnet covering these terrorists is the kind of dragnet the NSA would love to have on Americans, if Americans lost all concern for their privacy.

And that's just what the NSA (and GCHQ) have. The French have their own dragnet. They already had permission to hold onto metadata, but after the Charlie Hebdo attacks, they expanded their ability to wiretap without court approval. So the key ingredients to a successful use of the metadata were there: the ability to collect the metadata and awareness that one of the people was someone of concern.

The terrorists may have used encryption and therefore made it more difficult for authorities to get to the *content* of their Internet communications (though at this point, any iPhone encryption would only now be stalling investigators).

But their metadata should still have been available. There's no good way to hide metadata, which is why authorities find metadata dragnets so useful.

French authorities knew of at least one of these guys, and therefore would have been able to track his communication metadata, and both the Five Eyes and France have metadata dragnets restricted only by technology, and therefore might have been able to ID the network that carried out this attack.

Stewart Baker claims that Section 215 was designed to detect a plot like this. But the metadata dragnet covering France and the Middle East is even more comprehensive than Section 215 ever was. And it didn't detect the attack (it

also didn’t detect the Mumbai plot, even though — or likely because — one of our own informants was a key player in it). So rather than be a great argument for why we need to keep a dragnet that has never once prevented an attack in the US, Baker’s quip is actually proof that the dragnets don’t work as promised.