

ED FELTEN ON THE 30% COLLECTION CLAIM AND TECHNICAL DEBT

Ed Felten has his own take on last week's claims that the NSA was only collecting 30% of phone data.

He suggests my observation—which he calls an argument—that the dragnet combines data from multiple sources is unlikely because it would pose a great risk to NSA's credibility.

Theory A: Not under this program: One theory is that the NSA is actually getting a lot of domestic phone call data from another source, so this is another one of the “not under this program” evasions. This would mean the NSA is getting domestic phone call data via some method other than a Section 215 court order. For example, Marcy Wheeler argues that the data is coming from a foreign partner agency.

The argument against this theory is that it assumes the NSA is still willing to deceive the public and policymakers with the “not under this program” maneuver. The price to the agency's credibility of getting caught in such a trick at this late date would seem to be fairly high.

Of course, on the specific issue of geolocation (which the reports claim is part of the problem) the Administration has always engaged in this game (and was doing so as recently as October), assuring us they don't collect geolocation **under this program**.

More importantly, I think Felten misrepresents who might be misinformed. The issue, I believe, is not exclusively about misinformation (though there's some of that); it's about classification.

My observation is that the NSA collects a great deal of cell data under EO 12333 authorities – an observation backed by (among other sources) Snowden-released documents.

The question, then, is how much the NSA and ODNI are willing to talk about EO 12333 activities. And the answer to that has consistently been “unwilling.” As recently as October, James Clapper outright refused to answer an Amy Klobuchar question pertaining to EO 12333 authorities. When I asked former senior DNI official Jill Rhodes about EO 12333 collection last Friday – referring exclusively to information ODNI had declassified – she would not address that question either. We should assume that Intel Community sources will not discuss issues pertaining to EO 12333 – publicly at least– all the more so when they involve GCHQ involvement. I believe the Intelligence Committees have more information, but even there, Dianne Feinstein is quite clear that they have less oversight on EO 12333 activities than they do on FISA ones.

In addition, it’s worth noting that the **only way** Administration figures can have told the truth in all statements – both in their explicit claims to the Courts and Congress that they need the entire haystack and in their anonymous claims they only get 30% of phone data under Section 215 is if the haystack incorporates data from other sources as well. Which the public record shows to be the case.

All that said, I do think Felten’s explanation is part of what’s going on. He suggests the NSA may just have never properly solved some of the underlying problems they claim to be facing today.

Why might straightforward technical issues be holding up the program? One reason is that the program might be mired in technical debt.

For those not familiar with the concept, technical debt is a concept from

software engineering. If your project has an engineering problem to address, the “right” response is to understand the underlying cause and address it in a careful (yet cost-aware) fashion. Alternatively, you can slap on a quick and dirty “band-aid” solution that makes the problem go away in the short run but leaves the system more fragile and bug-prone. If you opt for the band-aid approach, you are taking on *technical debt*. Until you *pay back the principal* by addressing the underlying engineering problem, you will have to keep *paying interest on the debt* by devoting engineering effort to coping with extra crashes and bugs.

Although prudent managers take on technical debt at times, there is also a trap—as with financial debt—in which the burden of interest payments makes it more difficult to dig yourself out of debt, and your engineering staff spends all their time “putting out fires” rather than improving the product. Worst case, you can’t keep up with interest payments and can only pay the bills (i.e. keep the system alive) by taking on further debt. Then you slide into technical insolvency, where the system never really works right.

Government systems seem to be at higher risk of technical debt or insolvency, for reasons that would require another post to unpack.

This is why I said that some of the absurd claims peddled to the journalists have some grain of truth, such as the claim that crises in 2009 and 2013 prevented the NSA from fixing this problem. The claim is absurd if you believe the issue was seen as important in 2001 when NSA set up the dragnet or between 2006 and 2008 when NSA operated happily under FISC oversight or in 2011 to 2012 when the NSA was, in fact, working on

precisely the issues the leaked reports say underlie the difficulties.

But it's not absurd if the issue has been a problem primarily during those crisis periods when NSA didn't manage the issue.

And given that we know Verizon was having problems in 2009 pertaining to the mix of foreign and domestic records, I think it's safe to say that NSA kluged together solutions during the last crisis.

All that said, i suspect it is a technical debt created by legal debt, in part. While I think the issue here arises from legal arbitrage (the interest in doing what ever is most flexible under the law), I do think that may create technical issues (that should be a cinch to solve).