FBI HAS BEEN NOT COUNTING ENCRYPTION'S IMPACT ON INVESTIGATIONS FOR OVER A DECADE

During the first of a series of hearings in the last year in which Jim Comey (at this particular hearing, backed by Deputy Attorney General Sally Yates) pushed for back doors, they were forced to admit they didn't actually have numbers proving encryption was a big problem for their investigations because they simply weren't tracking that number.

> On the issue on which Comey — and his co-witness at the SJC hearing, Deputy Attorney General Sally Yates — *should* have been experts, they were not. Over an hour and a quarter into the SJC hearing, Al Franken asked for actual data demonstrating how big of a problem encryption really is. Yates replied that the government doesn't track this data because once an agency discovers they're targeting a device with unbreakable encryption, they use other means of targeting. (Which seems to suggest the agencies *have* other means to pursue the targets, but Yates didn't acknowledge that.) So the agencies simply don't count how many times they run into encryption problems. "I don't have good enough numbers yet," Comey admitted when asked again at the later hearing about why FBI can't demonstrate this need with real data.
>
> In point of fact, a recent wiretap report shows that in the criminal context, at least, federal agencies do count such incidences, sometimes. But they don't report the numbers in a

> timely fashion (5 of the 8 encrypted federal wiretaps reported in 2014 were from earlier years that were only then being reported), and agencies were eventually able to break most of the encrypted lines (also 5 of 8). Moreover, those 8 encrypted lines represented only 0.6 percent of all their wiretaps (8 of 1279). Reporting for encrypted state wiretaps were similarly tiny. Those numbers don't reflect FISA wiretaps. But there, FBI often partners with NSA, which has even greater ability to crack encryption.
>
> In any case, rather than documenting the instances where encryption thwarted the FBI, Comey instead asks us to just trust him.

Which is important background to an ancillary detail in this NYT story on how FBI tried a work-around for PGP in 2003 — its first attempt to do so — to go after some animal rights activists (AKA "eco-terrorists).

> In early 2003, F.B.I. agents hit a roadblock in a secret investigation, called Operation Trail Mix. For months, agents had been intercepting phone calls and emails belonging to members of an animal welfare group that was believed to be sabotaging operations of a company that was using animals to test drugs. But encryption software had made the emails unreadable.
>
> So investigators tried something new. They persuaded a judge to let them remotely, and secretly, install software on the group's computers to help get around the encryption.
>
> [snip]
>
> "This was the first time that the Department of Justice had ever approved such an intercept of this type," an

> F.B.I. agent wrote in a 2005 document summing up the case.

DOJ didn't include this encounter with encryption in the wiretap reports that mandate such reporting.

> It is also unclear why the Justice Department, which is required to report every time it comes across encryption in a criminal wiretap case, did not do so in 2002 or 2003. The Justice Department and F.B.I. did not comment Wednesday.

It didn't count that encounter with crypto even though FBI was discussing — as Bob Litt would 13 years later — exploiting fears of "terrorism" to get Congress to pass a law requiring back doors.

> "The current terrorism prevention context may present the best opportunity to bring up the encryption issue," an F.B.I. official said in a December 2002 email. A month later, a draft bill, called Patriot Act 2, revealed that the Justice Department was considering outlawing the use of encryption to conceal criminal activity. The bill did not pass.

Now, it may be that, as remained the case until last year, FBI simply doesn't record that they encountered encryption and instead tries to get the information some other way. But by all appearances, encryption was tied to that wiretap.

Which suggests another option: that FBI isn't tracking how often it encounters encryption because it doesn't want to disclose that it is actually finding a way around it.

That'd be consistent with what they've permitted providers to report in their transparency reports. Right now, providers are not permitted to report on new collection (say, collection

reflecting the compromise of Skype) for two years after it starts. The logic is that the government is effectively giving itself a two year window of exclusive exploitation before it will permit reporting that might lead people to figure out something new has been subjected to PRISM or other collection.

Why would we expect FBI to treat its own transparency any differently?

Update: This post has been updated to include more of the NYT article and a discussion of how encryption transparency may match provider transparency.