# FBI STILL NOT COUNTING HOW OFTEN ENCRYPTION HINDERS THEIR INVESTIGATIONS

The annual wiretap report is out. The headline number is that wiretaps have gone up, and judges still don't deny any wiretap applications.

> The number of federal and state wiretaps reported in 2015 increased 17 percent from 2014. A total of 4,148 wiretaps were reported as authorized in 2015, with 1,403 authorized by federal judges and 2,745 authorized by state judges. Compared to the applications approved during 2014, the number approved by federal judges increased 10 percent in 2015, and the number approved by state judges increased 21 percent. No wiretap applications were reported as denied in 2015.

The press has focused more attention on the still very small number of times encryption thwarts a wiretap.

> The number of state wiretaps in which encryption was encountered decreased from 22 in 2014 to 7 in 2015. In all of these wiretaps, officials were unable to decipher the plain text of the messages. Six federal wiretaps were reported as being encrypted in 2015, of which four could not be decrypted. Encryption was also reported for one federal wiretap that was conducted during a previous year, but reported to the AO for the first time in 2015. Officials were not able to decipher the plain text of the communications in that intercept.

Discussing the number — which doesn't include data at rest — on Twitter got me to look at something that is perhaps more interesting.

Back in July 2015, 7 months into the period reported on today, Deputy Attorney General Sally Yates and FBI Director Jim Comey testified in a "Going Dark" hearing. Over the course of the hearing, they admitted that they simply don't have the numbers to show how big a problem encryption is for their investigations, and they appeared to promise to start counting that number.

Around January 26, 2016 (that's the date shown for document creation in the PDF) — significantly, right as FBI was prepping to go after Syed Rizwan Farook's phone, but before it had done so — Comey and Yates finally answered the Questions for the Record submitted after the hearing. After claiming, in a response to a Grassley question on smart phones, "the data on the majority of the devices seized in the United States may no longer be accessible to law enforcement even with a court order or search warrant," Comey then explained that they do not have the kind of statistical information Cy Vance claims to keep on phones they can't access, explaining (over five months after promising to track such things),

> As with the "data-in-motion" problem, the FBI is working on improving enterprise-wide quantitative data collection to better explain the "data-at-rest" problem."
>
> [snip]
>
> As noted above, the FBI is currently working on improving enterprise-wide quantitative data collection to better understand and explain the "data at rest" problem. This process includes adopting new business processes to help track when devices are encountered that cannot be decrypted, and when we believe leads have been lost or investigations

> impeded because of our inability to obtain data.
>
> [snip]
>
> We agree that the FBI must institute better methods to measure these challenges when they occur.
>
> [snip]
>
> The FBI is working to identify new mechanisms to better capture and convey the challenges encountered with lawful access to both data-in-motion and data-at =-rest.

Grassley specifically asked Yates about the Wiretap report. She admitted that DOJ was still not collecting the information it promised to back in July.

> The Wiretap Report only reflects the number of criminal applications that are sought, and not the many instances in which an investigator is dissuaded from pursuing a court order by the knowledge that the information obtained will be encrypted and unreadable. That is, the Wiretap Report does not include statistics on cases in which the investigator does not pursue an interception order because the provider has asserted that an intercept solution does not exist. Obtaining a wiretap order in criminal investigations is extremely resource-intensive as it requires a huge investment in agent and attorney time, and the review process is extensive. It is not prudent for agents and prosecutors to devote resources to this task if they know in advance the targeted communications cannot be intercepted. The Wiretap Report, which applies solely to approved wiretaps, records only those extremely rare instances where agents and prosecutors obtain a wiretap order and are surprised

> when encryption prevents the court-ordered interception. It is also important to note that the Wiretap Report does not include data for wiretaps authorized as part of national security investigations.

These two answers lay out why the numbers in the Wiretap Report are of limited value in assessing how big a problem encryption is.

But they also lay out how negligent DOJ has been in responding to the clear request from SJC back in July 2015.