ON DECEMBER 10, INTELLIGENCE COMMITTEES NOT TOLD ANY ENCRYPTED COMMUNICATIONS USED IN SAN BERNARDINO

Here's what Senate Intelligence Chair Richard Burr and House Intelligence Ranking Member Adam Schiff had to say about a briefing on the San Bernardino attack they attended on December 10.

> Lawmakers on Thursday said there was no evidence yet that the two suspected shooters used encryption to hide from authorities in the lead-up to last week's San Bernardino, Calif., terror attack that killed 14 people.
>
> "We don't know whether it played a part in this attack," Senate Intelligence Committee Chairman Richard Burr (R-N.C.) told reporters following a closed-door briefing with federal officials on the shootings.
>
> But that hasn't ruled out the possibility, Burr and others cautioned.
>
> "That's obviously one issue were very interested in," House Intelligence Committee ranking member Adam Schiff (D-Calif.) said. "To what degree were either encrypted devices or communications a part of the impediment of the investigation, either while the events were taking place or to our investigation now?"
>
> The recent terror attacks in San Bernardino and Paris have shed an intense spotlight on encryption.
>
> While no evidence has been uncovered

> that either plot was hatched via secure communications platforms, lawmakers and federal officials have used the incidents to resurface an argument that law enforcement should have guaranteed access to encrypted data.

On December 10, we should assume from these comments, the Congressmen privy to the country's most secret intelligence and law enforcement information, were told nothing about a key source of evidence in the San Bernardino attack being encrypted. Schiff made it quite clear the members of Congress in the briefing were quite interested in that question, but nothing they heard in the briefing alerted them to a known trove of evidence being hidden by encryption.

That's an important benchmark because of details the FBI provided in response to a questions from Ars Tecnica's Cyrus Farivar. As had been made clear in the warrant, FBI seized the phone on December 3. But the statement also reveals that FBI asked the County to reset Farook's Apple ID password on December 6. That means they were already working on that phone several days before the briefing to the Intelligence Committee members (it's unclear whether that briefing was just for the Gang of Four or for both Intelligence Committees).

While, given what Tim Cook described last night, the FBI had not yet asked for Apple's assistance by that point, the FBI had to have known what they were dealing with by December 6 — an iPhone 5C running iOS9. Therefore, they would have known the phone was encrypted by default (and couldn't be open with a fingerprint).

Yet even four days later, they were not sufficiently interested in that phone they had to have known to be encrypted to tell Congress it held key data.

Update: Wow, this, from Apple's motion to vacate the order, makes this all the more damning.

5. On Saturday, December 5, 2015, Apple's emergency 24/7 call center received a call at approximately 2:46 a.m. PST requesting information relating to the case. Throughout that day, Apple employees were in regular communication with the FBI regarding its investigation. The same day, Apple received legal process seeking customer or subscriber information regarding three names and nine specific accounts. In response to that request, Apple made two productions of information that same day.