

CLASSIFIED BRIEFINGS: FOR WHEN YOUR PUBLIC CLAIMS DON'T HOLD UP TO SCRUTINY

As I laid out when he gave his speech at Brookings, Jim Comey's public explanation for needing back doors to Apple and Android phones doesn't hold up. He conflated stored communication with communication in transit, ignored the risk of a back door (which he called a front door), and the law enforcement successes he presented, across the board, do not support his claim to need a back door.

So yesterday Comey and others had a classified briefing, where no one would be able to shred his flawed case.

FBI and Justice Department officials met with House staffers this week for a classified briefing on how encryption is hurting police investigations, according to staffers familiar with the meeting.

The briefing included Democratic and Republican aides for the House Judiciary and Intelligence Committees, the staffers said. The meeting was held in a classified room, and aides are forbidden from revealing what was discussed.

[snip]

Comey called for Congress to revise the law to create a "level playing field" so that Google, Apple, and Facebook have the same obligation as AT&T and Verizon to help police.

National Journal listed out those companies, by the way – Facebook, for example, did not appear in Comey's Brookings speech where he used the "level the playing field comment."

I was puzzled by Comey's inclusion of Facebook here until I saw this news.

To make their experience more consistent with our goals of accessibility and security, we have begun an experiment which makes Facebook available directly over Tor network at the following URL:

<https://facebookcorewwwi.onion/>

[NOTE: link will only work in Tor-enabled browsers]

Facebook Onion Address

Facebook's onion address provides a way to access Facebook through Tor without losing the cryptographic protections provided by the Tor cloud.

The idea is that the Facebook onion address *connects you to Facebook's Core WWW Infrastructure* – check the URL again, you'll see what we did there – and it reflects one benefit of accessing Facebook this way: that it provides end-to-end communication, from your browser directly into a Facebook datacentre.

All that got me thinking about what Comey said in the classified briefing – in the real reason he wants to make us all less secure.

And I can't help but wonder whether it's metadata.

The government aspires to get universal potential coverage of telephony (at least) metadata under USA Freedom Act, with the ability to force cooperation. But I'm not sure that Apple, especially, would be able to provide iMessage metadata, meaning iPhone users can text without leaving metadata available to either AT&T (because it bypasses the telecom network) or Apple itself (because they no longer have guaranteed remote object).

And without metadata, FBI and NSA would be

unable to demonstrate the need to do a wiretap of such content.

Ah well, once again I reflect on what a pity it is that FBI didn't investigate the theft of data from these same companies, providing them a very good reason to lock it all up from sophisticated online criminals like GCHQ.