DOJ TO APPLE: START COOPERATING OR YOU'LL GET THE LAVABIT TREATMENT

DOJ has submitted its response to Apple in the Syed Farook case. Amid invocations of a bunch of ominous precedents — including Dick Cheney's successful effort to hide his energy task force, Alberto Gonzales effort to use kiddie porn as an excuse to get a subset of all of Google's web searches, and Aaron Burr's use of encryption — it included this footnote explaining why it hadn't just asked for Apple's source code.

> [9] For the reasons discussed above, the FBI cannot itself modify the software on Farook's iPhone without access to the source code and Apple's private electronic signature. The government did not seek to compel Apple to turn those over because it believed such a request would be less palatable to Apple. If Apple would prefer that course, however, that may provide an alternative that requires less labor by Apple programmers. *See In re Under Seal*, 749 F.3d 276, 281-83 (4th Cir. 2014) (affirming contempt sanctions imposed for failure to comply with order requiring the company to assist law enforcement with effecting a pen register on encrypted e-mail content which included producing private SSL encryption key).

That's a reference to the Lavabit appeal, in which Ladar Levison was forced to turn over its encryption keys.

As it happens, Lavabit submitted an amicus in this case (largely arguing against involuntary servitude). But as part of it, they revealed that the reason the government demanded Lavabit's key is because "in deference to [Edward Snowden's] background and skillset, the Government presumed the password would be impossible to break using brute force."

> Specifically, the Government sought to access encrypted e-mails stored on the Lavabit servers, which were impossible to access without a user's password. In contrast to the current situation, and in deference to the target's background and skillset, the Government presumed the password would be impossible to break using brute force. To overcome this barrier, the FBI sought the private encryption key used by Lavabit to protect the Secure Socket Layer ("SSL") and Transport Layer Security ("TLS") connections to their servers.

But that says that for phones that — unlike Farook's which had a simple 4-digit passcode — the government maintains the right to demand more, up to and including their source code.

The government spends a lot of time in this brief arguing it is just about this one phone. But that footnote, along with the detail explaining why they felt the need to obtain Lavabit's key, suggests it's about far more than even Apple has claimed thus far.