# UPDATE ON LAVABIT

I've been trying to keep an eye on the public information about the government's demand on Lavabit. And in a new interview with Ars Technica, Ladar Levison basically gives us a multiple choice guess on what the request was: either altering the source code or turning over the private key securing his HTTPS certificate.

> Levison said he has always known Lavabit safeguards could be bypassed if government agents took drastic measures, or as he put it, "if the government was willing to sacrifice the privacy of many to conduct surveillance on the few." For instance, if he was forced to change the code used when a user logs in, his system could capture the plain-text password needed to decrypt stored e-mails. Similarly, if he was ever forced to turn over the private encryption key securing his site's HTTPS certificate, government agents tapping a connection could observe the password as a user was entering it. But it was only in the past few weeks that he became convinced those risks were realistic.
>
> "I don't know if I'm off my rocker, but 10 years ago, I think it would have been unheard of for the government to demand source code or to make a change to your source code or to demand your SSL key," Levison told Ars. "What I've learned recently makes me think that's not as crazy an assumption as I thought."

I and others have suggested this (whichever of these options this demand took) is basically CALEA II — FBI's repeated demands that it have a back door into anything — before its time.

But Congress has not yet authorized CALEA II. So why did the (presumably) FISA Court approve this demand?