DOJ'S CLEAR THREAT TO GO AFTER APPLE'S SOURCE CODE

Oops: My post URLs crossed. Here's where If Trump's Protestors Didn't Exist He Would Have to Invent Them is.

In a rather unfortunate section heading the government used in their brief responding to Apple last week, DOJ asserted "There Is No Due Process Right Not to Develop Source Code." The heading seemed designed to make Lavabit's point about such requests being involuntary servitude.

I'd like to elaborate on this post to look at what DOJ has to say about source code — because I think the filing was meant to be an explicit threat that DOJ can — and may well, even if Apple were to capitulate here — demand Apple's source code.

The government's filing mentions "source code" ~~nine~~ ten different times [see update]. The bulk of those mentions appear in DOJ's rebuttal to Apple's assertion of a First Amendment claim about having to write code that violates its own beliefs, as in these three passages (there is one more purportedly addressing First Amendment issues I discuss below).

> Incidentally Requiring a Corporation to Add Functional Source Code to a Commercial Product Does Not Violate the First Amendment
>
> Apple asserts that functional source code in a corporation's commercial product is core protected speech, such that asking it to modify that software on one device—to permit the execution of a lawful warrant—is compelled speech in violation of the First Amendment.
>
> [snip]
> There is reason to doubt that functional

> programming is even entitled to traditional speech protections. See, e.g., Universal City Studios, Inc. v. Corley, 273 F.3d 429, 454 (2d Cir. 2001) (recognizing that source code's "functional capability is not speech within the meaning of the First Amendment").
>
> [snip]
>
> To the extent Apple's software includes expressive elements—such as variable names and comments—the Order permits Apple to express whatever it wants, so long as the software functions. Cf. Karn v. United States Department of State, 925 F. Supp. 1, 9- 10 (D.D.C. 1996) (assuming, without deciding, that source code was speech because it had English comments interspersed).

Most people aside from EFF think Apple's First Amendment claim is the weakest part of its argument. I'm not so sure that, in the hands of the guy who argued Citizens United before SCOTUS, it will end up that weak. Nevertheless, DOJ focused closely on it, especially as compared to its treatment of Apple's Fifth Amendment argument, which is where that dumb heading came in. This is the entirety of DOJ's response to that part of Apple's argument.

> There Is No Due Process Right Not to Develop Source Code
>
> Apple lastly asserts that the Order violates its Fifth Amendment right to due process. Apple is currently availing itself of the considerable process our legal system provides, and it is ludicrous to describe the government's actions here as "arbitrary." (Opp. 34); see County of Sacramento v. Lewis, 523 U.S. 833, 846-49 (1998). If Apple is asking for a Lochner-style holding that businesses have a substantive due

> process right against interference with its marketing strategy or against being asked to develop source code, that claim finds no support in any precedent, let alone "in the traditions and conscience of our people," "the concept of ordered liberty," or "this Nation's history." Washington v. Glucksberg, 521 U.S. 702, 721 (1997).

Though admittedly, that's about how much Apple included in its brief.

> The Fifth Amendment's Due Process Clause Prohibits The Government From Compelling Apple To Create The Request [sic] Code
>
> In addition to violating the First Amendment, the government's requested order, by conscripting a private party with an extraordinarily attenuated connection to the crime to do the government's bidding in a way that is statutorily unauthorized, highly burdensome, and contrary to the party's core principles, violates Apple's substantive due process right to be free from "'arbitrary deprivation of [its] liberty by government.'" Costanich v. Dep't of Soc. & Health Servs., 627 F.3d 1101, 1110 (9th Cir. 2010) (citation omitted); see also, e.g., Cnty. of Sacramento v. Lewis, 523 U.S. 833, 845-46 (1998) ("We have emphasized time and again that '[t]he touchstone of due process is protection of the individual against arbitrary action of government,' . . . [including] the exercise of power without any reasonable justification in the service of a legitimate governmental objective." (citations omitted)); cf. id. at 850 ("Rules of due process are not . . . subject to mechanical application in unfamiliar territory.").

In other words, both Apple and DOJ appear to

have a placeholder for discussions about takings (one that Lavabit argued from a Thirteenth Amendment perspective).

Those constitutional arguments, however, all seem to pertain the contested order requiring Apple to create source code that doesn't currently exist. Or do they?

As I noted in my earlier Lavabit post, the DOJ argument doesn't focus entirely on writing code that doesn't already exists. As part of its argument for necessity, DOJ pretends to take Apple at its word that the US government could not disable the features (as if that's what they would do if they had source code!) themselves.

> Without Apple's assistance, the government cannot carry out the search of Farook's iPhone authorized by the search warrant. Apple has ensured that its assistance is necessary by requiring its electronic signature to run any program on the iPhone. Even if the Court ordered Apple to provide the government with Apple's cryptographic keys and source code, Apple itself has implied that the government could not disable the requisite features because it "would have insufficient knowledge of Apple's software and design protocols to be effective." (Neuenschwander Decl. ¶ 23.)

Note DOJ claims to source that claim to Apple Manager of User Privacy Erik Neuenschwander's declaration (which is included with their motion). But he wasn't addressing whether the government would be able to reverse-engineer Apple's source code *at all*. Instead, that language came from a passage where he explained why experienced engineers would have to be involved in writing the new source code.

> New employees could not be hired to perform these tasks, as they would have insufficient knowledge of Apple's

> software and design protocols to be effective in designing and coding the software without significant training.

So the discussion of what the government could do with if it had Apple's source code is just as off point as the passage invoking the Lavabit case (which involved an SSL key, but not source code). Here's that full passage:

> The government has always been willing to work with Apple to attempt to reduce any burden of providing access to the evidence on Farook's iPhone. See Mountain Bell, 616 F.2d at 1124 (noting parties' collaboration to reduce perceived burdens). Before seeking the Order, the government requested voluntary technical assistance from Apple, and provided the details of its proposal. (Supp. Pluhar Decl. ¶ 12.) Apple refused to discuss the proposal's feasibility and instead directed the FBI to methods of access that the FBI had already tried without success. (Compare Neuenschwander Decl. ¶¶ 54-61, with Supp. Pluhar Decl. ¶ 12.) The government turned to the Court only as a last resort and sought relief on narrow grounds meant to reduce possible burdens on Apple. The Order allows Apple flexibility in how to assist the FBI. (Order ¶ 4.) The government remains willing to seek a modification of the Order, if Apple can propose a less burdensome or more agreeable way for the FBI to access Farook's iPhone.9
>
> 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).

Effectively, having invented a discussion about whether the government would be able to use Apple's source code out of thin air, DOJ returns to that possibility here, implying that that would be the least burdensome way of getting what it wanted and then reminding that it has succeeded in the past in demanding that a provider expose all of its users to government snooping, even at the cost of shutting down the business, even after Ladar Levison (after some complaining) had offered to provide decrypted information himself.

Significantly, the government obtained a warrant for Lavabit's keys as a way of avoiding the question of whether the "technical assistance" language in the Pen/Trap statute extended to sharing keys, but Levison was ultimately held in contempt for all the orders served on him, including the Pen/Trap order and its language about technical assistance. The Fourth Circuit avoided ruling on whether that assistance language in Pen/Trap orders extended to encryption keys by finding that Levison had not raised it prior to appeal and that the District Court had not clearly erred, which effectively delayed consideration of the same kinds of issues at issue (though under a different set of laws) in the Apple encryption cases.

> In making his statement against turning over the encryption keys to the Government, Levison offered only a one-sentence remark: "I have only ever objected to turning over the SSL keys

> because that would compromise all of the secure communications in and out of my network, including my own administrative traffic." (J.A. 42.) This statement — which we recite here verbatim — constituted the sum total of the only objection that Lavabit ever raised to the turnover of the keys under the Pen/Trap Order. We cannot refashion this vague statement of personal preference into anything remotely close to the argument that Lavabit now raises on appeal: a statutory-text-based challenge to the district court's fundamental authority under the Pen/Trap Statute. Levison's statement to the district court simply reflected his personal angst over complying with the Pen/Trap Order, not his present appellate argument that questions whether the district court possessed the authority to act at all.
>
> [snip]
>
> The Government, however, never stopped contending that the Pen/Trap Order, in and of itself, also required Lavabit to turn over the encryption keys. For example, the Government specifically invoked the Pen/Trap Order in its written response to Lavabit's motion to quash by noting that "four separate legal obligations" required Lavabit to provide its encryption keys, including the Pen/Trap Order and the June 28 Order.
>
> [snip]
>
> In view of Lavabit's waiver of its appellate arguments by failing to raise them in the district court, and its failure to raise the issue of fundamental or plain error review, there is no cognizable basis upon which to challenge the Pen/Trap Order. The district court did not err, then, in

> finding Lavabit and Levison in contempt once they admittedly violated that order.

In other words, the Lavabit reference, like the invention of an Apple discussion about what the government could do with its source code (any such discussion would have been interesting in and of itself, because I'd bet Apple would be more confident FBI couldn't do much with its source code than that NSA couldn't), was off point. But in introducing both references, DOJ laid the groundwork for a demand for source code to be the *fallback, least burdensome* position.

And, as I noted, in the Lavabit case, the government justified demanding a key based on the presumption that Edward Snowden would have a more complicated password than Syed Rizwan Farook's 4-digit numerical passcode. That is, in that case, the government tied a more intrusive demand to the difficulty of accessing a target's communications, not to the law itself, which suggests they'd be happy to do so in the future if they were faced with an Apple phone with a passcode too complex to brute force in 26 minutes, as FBI claims it could do here.

All of which brings me to one more citation of source code in DOJ's extended First Amendment discussion: a reference to a civil case where Apple was able to obtain the source code of a competitor.

> This form of "compelled speech" runs throughout both the criminal and civil justice systems, from grand jury and trial subpoenas to interrogatories and depositions. See, e.g., Apple Inc.'s Motion to Compel in Apple Inc. v. Samsung Electronics, Docket No. 467 in Case No. 11–cv–1846–LHK, at 11 (N.D. Cal. Dec. 8, 2011) (Apple's seeking court order compelling Samsung to produce source code to facilitate its compelled deposition of witnesses about that source code).

Note, this is not a case about Apple (or Samsung, in this case) being compelled to write new code at all. Rather, it is a case about handing over the source code a company already had. In another off point passage, then, DOJ pointed to a time when Apple itself successfully argued the provision of source code could be compelled, even in a civil case.

Through a variety of means, DOJ went well out of its way to introduce the specter of a demand for Apple's source code into its response. They are clearly suggesting that if Apple refuses to write code that doesn't exist, the government will happily take code that does.

Loretta Lynch claimed, under oath last week, that the government doesn't want a back door into Apple products. That's not what her lawyers have suggested in this brief. Not at all.

Update: Here's how Apple treated this in its Reply:

> The government also implicitly threatens that if Apple does not acquiesce, the government will seek to compel Apple to turn over its source code and private electronic signature. Opp. 22 n.9. The catastrophic security implications of that threat only highlight the government's fundamental misunderstanding or reckless disregard of the technology at issue and the security risks implicated by its suggestion.

Also, in writing this post, I realized there's one more reference to source code in the government's Response, one that admits Apple's source code is "the keys to the kingdom."

> For example, Apple currently protects (1) the source code to iOS and other core Apple software and (2) Apple's electronic signature, which as described above allows software to be run on Apple hardware. (Hanna Decl. Ex. DD at 62-64

> (code and signature are “the most confidential trade secrets [Apple] has”).) *Those* —which the government has *not* requested—are the keys to the kingdom. If Apple can guard them, it can guard this.