JUST SECURITY
A FORUM ON LAW, RIGHTS, AND U.S. NATIONAL SECURITY

Feinstein-Burr, Encryption and the "Rule of Law"

Julian Sanchez

April 19, 2016

There's a lot to say about the substance of the misguided anti-encryption legislation sponsored by Sens. Dianne Feinstein and Richard Burr, which was recently released as a "discussion draft" after a nearly-identical version leaked earlier this month. I hope to do just that in subsequent posts. But it's also worth spending a little time on the proposal's lengthy pre-amble, which echoes the rhetorical tropes frequently deployed by advocates for mandating government access to secure communications and stored data.

The bill is somewhat misleadingly titled the "Compliance With Court Orders Act of 2016″—which you'd think would be a matter for the Judiciary Committee, not the Senate Select Committee on Intelligence—and begins with the high minded declaration that "no person or entity is above the law." Communictions services and software developers, we are told, must "respect the rule of law and comply with all legal requirements and court orders." In order to "uphold the rule of law," then, those persons and entities must be able to provide law enforcement with the plaintext—the original, ungarbled contents—of any encrypted message or file when so ordered by a court.

The politest way I can think of to characterize this way of framing the issue is: Nonsense. Whatever your view on mandates of the sort proposed here, they have little to do with the principle of "the rule of law": The idea that all citizens, including those who wield political power, must be governed by neutral, publicly known, and uniformly applicable rules—as opposed to, say, the whims and dictates of particular officials. This formal principle says nothing about the *content* of the legal obligations and restrictions to which citizens are subject—only that those restrictions and obligations, whatever they are, should be known and consistently applied. In effect, Feinsten and Burr are pretending that a sweeping and burdensome new regulatory requirement is nothing more than the application of a widely-revered formal principle central to free societies. We can debate the merits of their proposed regulation, but this talking point really ought to be laughed out of the room.

There are two wholly different kind of scenarios in which technology companies have recently been charged with placing themselves "above the law" by declining to assist law

enforcement. Both are specious, but it's worth distinguishing them and analyzing them separately.

First, you have the kind of situation at issue in the recent conflict between Apple and the FBI, which has received so much media coverage. In this instance, it is clear that Apple was indeed capable of doing what the FBI wanted it to do: Write a custom piece of software that would disable certain security features on the work iPhone used by a deceased terrorist, enabling the FBI to crack the phone's passcode and unlock the data within. Sen. Feinstein condemned the company for fighting that order in court, declaring: "Apple is not above the laws of the United States, nor should anyone or any company be above the laws. To have a court warrant granted, and Apple say they are still not going to cooperate is really wrong." A similar view of the conflict was implict in a slew of lazy news headlines that characterized Apple as "defying" a court's order.

All of this, however, reflects a profound and rather disturbing misunderstanding of how our legal system operates. Subpoenas and court orders routinely issue *initially* in response to a request from the government, with no opposing arguments heard. But the recipients of those orders, as a matter of course, have an essential legal right to contest those orders in an adversarial hearing. Here, Apple raised a variety of different objections—among them, that the statute invoked by the government, the All-Writs Act, did not actually authorize orders of the sort that the FBI had sought; and that even if the statute *could* be generally interpreted to permit such orders, that this one imposed an excessive and unreasonable burden on Apple.

Now, you can agree or disagree with the various legal arguments advanced by Apple, as well as the many legal and technical experts who lined up to back the company. But this is not Tim Cook standing atop a barricade howling "Anarchy!"—and it is a borderline-Orwellian abuse of language to say that a company puts itself "above the law" by *using the legal process* to contest the government's interpretation of the law. If the case had gone to the Supreme Court, Apple had lost, and still insisted it wouldn't comply, then yes, they'd be placing themselves "above the law." Until then, they're just working appropriately within the legal system, and it's frankly chilling to hear elected officials implying there's anything improper about that. "The rule of law" does not require that everyone engaged in litigation with the government should surrender and defer to the interpretation of the government's lawyers—especially given that one judge has already held that Apple has the better argument.

The second scenario the bill aims to address is the one where a company simply *can't* do anything to help, because they don't have access to the cryptographic keys needed to decipher a given message or file. Now, you can argue the merits of passing a new mandate requiring companies to have this capability. What you cannot reasonably argue is that "the rule of law" is undermined when, in the absence of a mandate, companies cannot comply with orders to decrypt files with user-generated keys. The rule of law does not mean that every imaginable outcome a

judge directs—from decrypting data to flying like a bird—must be achievable by anyone served with a court order.

Consider: It is possible to build cars (and, presumably, laptops or firerarms or any number of other consumer goods) with a GPS location beacon and a remote shutoff switch that will disable them until police can arrive in the event of theft. Some cars are indeed built with such features, which would no doubt be of great help to police in a variety of cases. But most cars are not built with these features, and nobody thinks General Motors—served with an order to locate a stolen car and shut down the engine—would be "defying the rule of law" if they had to reply: "We have no way to do that; we didn't build that car with those capabilities." Moreover, if a legislator proposed a massive and costly new regulation requiring that all new cars be built with such features, we would rightly gawp incredulously at the suggestion that this was merely an effort to "ensure compliance with court orders," as though the failure to build a feature useful to police were tantamount to obstruction of a lawful search warrant. We would, indeed, probably regard such an argument as a rather brazen attempt to downplay the costly new regulatory burden such a mandate would impose on auto makers.

All sorts of technologies—from document shredders to toilets—may help criminals keep incriminating material out of the hands of police. As a result, some searches conducted pursuant to lawful warrants will not succeed in turning up the evidence sought. We can regard that as unfortunate, and we can debate what measures what may be appropriate in aiding police meet with greater success. But anyone who tried to ratchet up the rhetoric by claiming that toilets therefore undermine the Rule of Law would be laughed out of the room—which is the appropriate reaction here, as well.

So much for rhetoric. In a subsequent post, I'll get into why the substantive idea of a "decryptability" mandate is so insanely misguided.

Julian Sanchez is a senior fellow at the Cato Institute and studies issues at the busy intersection of technology, privacy, and civil liberties, with a particular focus on national security and intelligence surveillance.