THE COSTS OF POLITICALLY FREE CYBERSECURITY FAILURES

Ben Wittes looks at the WaPo article and accompanying National Security Council Draft Options paper on how the White House should respond to FBI's campaign against encryption and declares that "Industry has already won."

> [T]he document lays out three options for the administration—three options that notably do *not* include seeking legislation on encryption.
>
> They are:
>
> - *"Option 1: Disavow Legislation and Other Compulsory Actions";*
> - *"Option 2: Defer on Legislation and Other Compulsory Actions"; and*
> - *"Option 3: Remain Undecided on Legislation or Other Compulsory Actions."*
>
> In all honesty, it probably doesn't matter all that much which of these options Obama chooses. If these are the choices on the table, industry has already won.

What's most fascinating about the white paper is that it lays bare how the NSC itself sees this issue – and they don't see it like Wittes does, nor in the way the majority of people clamoring for back doors have presented it. As the NSC

defines the issue, this is not "industry" versus law enforcement. For each assessed scenario, NSC measures the impact on:

- Public safety and national security
- Cybersecurity
- Economic competitiveness
- Civil liberties and human rights

Arguably, there's a fifth category for each scenario — foreign relations — that shows up in analysis of reaction by stakeholders that weighs the interests of foreign governments, including allies that want back doors (UK, France, Netherlands), allies that don't (Germany and Estonia), and adversaries like Russia and China that want back doors to enable repression (and, surely, law enforcement, but the analysis doesn't consider this).

That, then, is the real network of interests on this issue and not — as Wittes, Sheldon Whitehouse, and many though not all defenders of back doors have caricatured — simply hippies and Apple versus Those Who Keep Us Safe.

NSC not only judges the market demand for encryption — and foreign insistence that US products not appear to be captive to America's national security state — to be real, but recognizes that those demands underlie US economic competitiveness generally.

And, as a number of people point out, the NSC readily admits that encryption helps cybersecurity. As the white paper explains,

> Pro-encryption statements from the government could also encourage broader use of encryption, which would also benefit global cybersecurity. Further, because any new access point to encrypted data increases risk, eschewing mandated technical changes ensures the greatest technical security. At the same

> time, the increased use of encryption could stymie law enforcement's ability to investigate and prosecute cybercriminals, though the extent of this threat over any other option is unclear as sophisticated criminals will use inaccessible encryption.

Shorter the NSC: If encryption is outlawed, only the sophisticated cyber-outlaws will have encryption.

This is the discussion we have not been having, as Jim Comey repeatedly talks in terms of Bad Guys and Good Guys, the complex trade-offs that are far more than "safety versus privacy."

What's stunning, however, is that NSC — an NSC that was already in the thick of responding to the OPM hack when this paper was drafted in July — sees cybersecurity as a separate category from public safety and national security. Since 2013, the Intelligence Community has judged that cybersecurity is a bigger threat than terrorism (though I'm not sure if the IC has revised that priority given ISIS' rise). Yet the NSC still thinks of this as a separate issue from public safety and national security (to say nothing of the fact that NSC doesn't consider the crime that encryption would prevent, such as smart phone theft).

I'm not surprised that NSC considers these different categories, mind you. Cybersecurity failures are still considered (with the sole exception of Katherine Archuleta, who was forced to resign as OPM head after the hack) politically free, such that men like John Brennan (when he was Homeland Security Czar *on* NSC) and Keith Alexander can have, by their own admission, completely failed to keep us safe from cyberattack without being considered failures themselves (and without it impacting Brennan's perceived fitness to be CIA Director).

The political free ride cybersecurity failures

get is a problem given the other reason that Wittes' claim that "industry has already won" is wrong. WaPo reports that NSC still hasn't come up with a preferred plan, ostensibly because it is so busy with other things.

> Some White House aides had hoped to have a report on the issue to give to the president months ago. But "the complexity of this issue really makes it a very challenging area to arrive at any sort of policy on," the senior official said. A Cabinet meeting to be chaired by National Security Adviser Susan Rice, ostensibly to make a decision, initially was scheduled for Wednesday, but it has been postponed.
>
> The senior official said that the delays are due primarily to scheduling issues — "there are a lot of other things going on in the world" — that are pressing on officials' time.

But WaPo also presents evidence that those who want back doors are just playing for time, until some kidnapping or terrorist attack investigation gets thwarted by encryption.

> Although "the legislative environment is very hostile today," the intelligence community's top lawyer, Robert S. Litt, said to colleagues in an August e-mail, which was obtained by The Post, "it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."
>
> There is value, he said, in "keeping our options open for such a situation."

So long as the final decision never gets made, those who want back doors will be waiting for the moment when some event changes the calculus that currently weighs in favor of encryption. And, of course, we'll all be relying on people

like Jim Comey to explain why encryption made it impossible to catch a "bad guy," which means the measure will probably ignore the other ways law enforcement can get information.

We are still living in Dick Cheney's world, where missing a terrorist attack (other than the big one or the anthrax attack) is assumed to be career ending, even while failing to address other threats to the US (climate change and increasingly cybersecurity) are not. So long as that's true, those waiting to use the next spectacular failure to make ill-considered decisions about back doors will await their day, putting some kinds of national security above others.

Update: Like me, Susan Landau thinks Wittes misunderstood what the White Paper said about who "won" this fight.

> But the National Security Council draft options paper never mentions national-security threats as a concern in the option of disavowing legislation controlling encryption (it does acknowledge potential problems for law enforcement). The draft says that no-legislation approach would help foster "the greatest technical security." That broad encryption use is in our national security interest is why the administration is heading to support the technology's broad use. That's the story here — and not the one about Silicon Valley.