# THE TWO LEGITIMACY PROBLEMS WITH THE NGHIA PHO SENTENCE

Nghia Pho was sentenced to 5 years and 6 months yesterday. He is presumed to have been one of the sources for the files released by Shadow Brokers (though I have been told he couldn't be the sole source).

The government had asked for 8 years, just a month short of the top of the guidelines for the crime to which he pled guilty (though the government could have charged him much more aggressively and gotten far more time). In sentencing Pho, however, Judge George Russell seemed persuaded by Pho attorney Robert Bonsib's point that David Petraeus did no jail time for what actually would have been a worse offense had he also been charged with sharing with his mistress the code word intelligence he mishandled and then lying about both to the FBI, as well as if the government admitted that the information Petraeus shared actually did show up in Paula Broadwell's hagiography of the general.

> Russell seemed particularly perturbed that former CIA Director David Petraeus managed to get probation after admitting he kept highly classified information in his home without permission, shared it with his girlfriend and lied to investigators.
>
> "Did he do one day in prison?" the clearly frustrated judge asked. "Not one day. … What happened there? I don't know. The powerful win over the powerless? … The people at the top can, like, do whatever they want to do and walk away."

Admittedly, the unstated presumption that Pho's mishandling of NSA's hacking tools led to first their leak then the downstream malware attacks

tied to them seems to justify the government's call for a harsh sentence and is reflected in statements from both Russell and prosecutor.

> Russell called Pho's actions "extraordinarily serious." He also rejected claims that it was an isolated mistake, noting that Pho took the top-secret material to his home for years.
>
> [snip]
>
> Little was said at Tuesday's hearing about what information may have escaped Pho's control or where it wound up, although Windom used very strong language about the impact of Pho's actions, calling it "devastating."

And it also explains the language of Pho's remorse — denying the things that might have been suspected of the release.

> "I admit it but I do not betray the U.S.A.," the white-haired, glasses-wearing engineer said in broken English. "I do not betray this country. … I do not send anything to anybody or on the internet. I do not make profit on this information. … I cannot damage this country."

It also might explain the terms of the plea agreement, one part of which remains sealed.

There's something that remains unexplained, however — at least not credibly. Pho continues to claim that he brought the NSA's hacking tools home because he needed them to write his Employee Performance Assessments. (h/t Josh Gerstein for obtaining the documents)

> I need extra times and information about what I worked on, cut and paste, to create a good EPA at home and hope that I will have a chance to be promoted this time hence I received a good high-three average salaries before I go to the

> retirement in next four years (2019) when my clearance will be expired.
>
> I was devoted to EPA promotion, encircle by EPA/promotion and the last high-three salaries that made me blind to violate the security policy of the Agency.

But as the government noted in their sentencing memo, this was not a one-off in advance of writing a yearly EPA. Rather, Pho continued doing this over the course of five years, *and did so with materials unrelated to his work.*

> For a period of at least five years, the defendant removed Top Secret and Sensitive Compartmented Information ("SCI") from secure space at the National Security Agency ("NSA") and retained it in his home—an unsecure residence.
>
> [snip]
>
> This assertion [that he did this solely for EPAs] is belied by the facts. The defendant did not take home and retain classified information consistently for five years to work on an annual performance review. This argument especially does not apply to the classified material found in his home that was unrelated to his work or any personnel evaluation. [citations removed]

The government also notes that Pho knew better than to load these materials onto his computer (as a guy who coded malware, that should be all the more true).

> The defendant claims that he stored massive troves of classified information at his home without the intention of placing national security at risk. The defendant goes so far as to say, directly, that he "did handle the

> information with care." His actions speak to his intentions, and the facts do not support his contentions. For years, the defendant received training on how and where to store classified information and on why such precautions were critical to protecting national security. The defendant well knew that the mere removal of classified information from secure spaces, in itself, could endanger national security, and that retaining classified information in an unsecure location compounded this danger. Indeed, in his plea agreement, the defendant admitted that his extensive training informed him that "unauthorized removal of classified materials and transportation and storage of those materials in unauthorized locations risked disclosure and transmission of those materials, and therefore could endanger the national security of the United States and the safety of its citizens.

This is a point that Admiral Rogers repeated in his (March 5) letter on the sentencing.

Mind you, even a year after Pho was discovered, it was still possible for even a translator to stick thumb drives into Top Secret computers at Fort Meade, as evidenced by Reality Winner's actions (actions that were not charged). In the same way that Pho knew well that putting hacking tools on a computer attached to the Internet would be colossally stupid, the government itself has known the risks of leaving computers accessible to removable media since before Chelsea Manning's leaks. They're not exactly in a position to lecture.

That said, there's something that still doesn't add up about this and Pho's claimed motive for it, which may be why when this story first broke, three different theories for why he brought the files home got leaked to the press. Maybe it was just ego fed by resentment that he

(as reported in his letter) wasn’t getting promotions at the same rate as his colleagues, which doesn’t make for a very good excuse to having exposed the NSA’s crown jewels.