SNOWDEN NEEDS A BETTER PUBLIC INTEREST DEFENSE: DISPOSING OF THE JOURNALIST FILTER

Some weeks ago, I wrote what was meant to be the second part of a three part review of Edward Snowden's book, *Permanent Record*, in which I argued that his use of the Bildungsroman genre raised more questions than it answered about the timing of the moment he came to decide to reveal NSA's files. I argued that the narrative did not present a compelling story that he had the maturity or the knowledge of the NSA's files needed to sustain a public interest defense before the time he decided to take those files.

I've been struggling to write what was meant to be the first part of that review. That first part was meant to assess what I will treat as Snowden's "cosmopolitan defense," showing that his leaks have since been judged by neutral authorities to have revealed legal or human rights violations. As that first part has evolved, it has shifted into a more of a reflection on the failures of the surveillance community as a whole (and therefore my own failures) and of limits to an investment in whistleblowing as exposure. That part is not ready yet, but I hope the release of the FISA IG Report tomorrow will serve as a sounding board to pull those thoughts together.

But since this, the intended third part of the review, was mostly done, I wanted to release it to get it out of the way.

In addition to my other reactions about how this book fails to offer what Snowden has always claimed he wanted to do — offer a defense that he leaked the files in the public interest that could withstand cross-examination — *this book*

harms the version of public interest defense Snowden has always offered. Snowden says that by sharing the NSA files with journalists, he made sure he wasn't imposing his judgment for society. Given how unpersuasive his explanation for picking (especially) Glenn Greenwald as the journalist to make those choices is, which I addressed in my last post, and given Glenn's much-mocked OpSec failures, there's only so far Snowden can take that claim, because it's always possible adversaries will steal the files or already have from journalists. *The Intercept*, in particular, went through very rigorous efforts to keep those files secure, but it took them some time to implement and that's just one set of the files that are out there.

Still, it is a claim that has a great deal of merit. It distinguishes Snowden from WikiLeaks. It mitigates a lot of concerns about the vast quantity of documents he took (or the degree to which they may relate to core national security concerns). I'm a journalist who once lost a battle to release Snowden documents that showed a troubling use of NSA authorities and who a second time chose not to rely on a Snowden document because its demonstrative value did not overcome the security damage releasing it might do. My experience working directly with the Snowden files is really quite limited and rather comical in its frustrations, but I will attest that there was a rigorous process put in place to protect the files and assess whether or not to publish them.

So I'm utterly biased about the value that journalists' judgment might have served here. But if it ever comes to it, I will happily explain at length how Snowden's choice to leak to journalists really does distinguish his actions.

Having made that argument, though, Snowden then violates precisely that principle by writing this book.

There hasn't been a lot of discussion about the disclosures Snowden makes *in this book*. They

pale in comparison to what got disclosed with his NSA files. Nevertheless, I'm certain that Snowden revealed things that have forced CIA to mitigate risks if they hadn't already done so before the book came out. In particular, Snowden describes the infrastructure of four different IC facilities, mostly CIA ones, in a way that would be useful for adversaries. Sure, our most skilled adversaries likely already knew what he disclosed in the book, but this book makes those details (if they haven't already been mitigated) accessible to a wider range of adversaries.

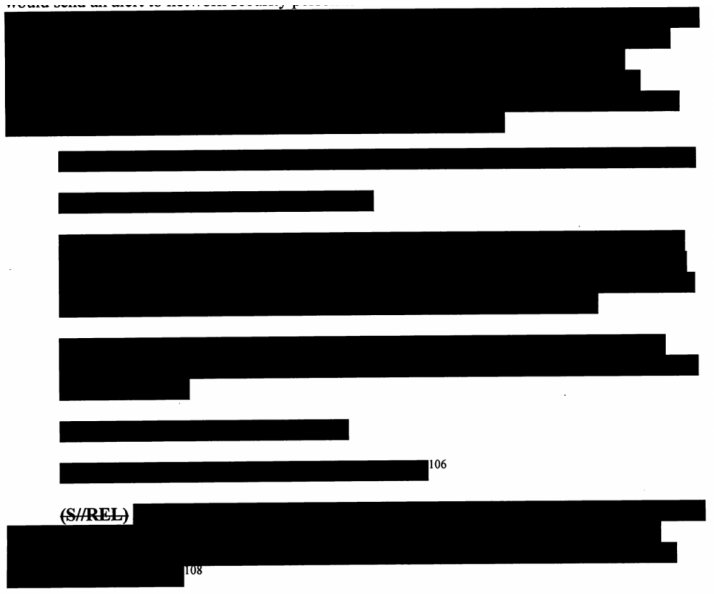
More curious still is what Snowden makes a big show of not disclosing. In the book, Snowden describes how he took the files. While he describes sneaking the NSA's files out on SD cards, he pointedly doesn't explain how he transferred the files onto those SD cards.

> I'm going to refrain from publishing how exactly I went about my own writing—my own copying and encryption—so that the NSA will still be standing tomorrow.

If Snowden really is withholding this detail out of some belief that sharing it would bring the NSA down tomorrow, he effectively just put a target on his back, walking as that back is around Moscow, to be coerced to answer precisely this question. And if Snowden really believes this detail is that damaging to the NSA, his assurances that he destroyed his encryption key to the files before he left Hong Kong and so could not be coerced, once he arrived in Russia, to share damaging information on the US falls flat. By his own estimation, Snowden did not destroy some of the most valuable knowledge he had that might be of interest, information he claims could bring the NSA down tomorrow.

I actually doubt that's why he's withholding that detail. After all, the HPSCI Report on Snowden has a three page section that describes this process, including this entirely redacted passage (PDF 18) describing a particular vulnerability he used to make copies of the

files, one the unredacted part of the HPSCI report suggests may have been unknown to NSA when Snowden exploited it.



~~(S//REL)~~ There is no evidence that NSA was aware of this specific vulnerability to its networks. Because Snowden's legitimate work responsibilities involved transferring large amounts of data between different SharePoint servers, the large quantities of data he copied as Step 1 of the exfiltration process did not trigger any NSA alerts for abnormal network traffic.[109]

Assuming the NSA, focusing all its forensic powers on understanding what had been, to that point, the agency's worst breach ever, managed to correctly assess the vulnerability Snowden used by October 29, 2014, the date the NSA wrote a report describing "Methods Used by Edward Snowden To Remove Documents from NSA Networks," then the NSA has presumably already fixed the vulnerability.

I honestly don't know why, then, Snowden kept that detail secret. It's possible it's something banal, an effort to avoid sharing the critical forensic detail that would be used to prosecute him if he ever were to stand trial (though it's not like there's any doubt he took the documents). I can think of other possible reasons, but *why* he withheld this detail is a big question about the choices he made about what to disclose and what not to disclose in this book.

But that's the challenge for Snowden, after investing much of a public interest defense in using journalists as intermediaries, now making choices personally about what to disclose and

what to withhold. It accords Snowden a different kind of responsibility for the choices he makes in this book. And it’s not clear that, having assumed that role, Snowden met his own standards.