HPSCI: WE MUST SPY LIKE SNOWDEN TO PREVENT ANOTHER SNOWDEN

I was going to write about this funny part of the HPSCI report anyway, but it makes a nice follow-up to my post on Snowden and cosmopolitanism, on the importance of upholding American values to keeping the servants of hegemon working to serve it.

As part of its attack on Edward Snowden released yesterday, the House Intelligence Committee accused Snowden of attacking his colleagues' privacy.

> To gather the files he took with him when he left the country for Hong Kong, Snowden infringed on the privacy of thousands of government employees and contractors. He obtained his colleagues' security credentials through misleading means, abused his access as a systems administrator to search his co-workers' personal drives, and removed the personally identifiable information of thousands of IC employees and contractors.

I have no doubt that many — most, perhaps — of Snowden's colleagues feel like he violated their privacy, especially as their identities are now in the possession of a number of journalists. So I don't make light of that, or the earnestness with which HPSCI's sources presumably made this complaint (though IC employee privacy is one of the things all journalists who have reported these stories have redacted, to the best of my knowledge).

But it's a funny claim for several reasons. Even ignoring that what the NSA does day in and day out is search people's personal communications

(including millions of innocent people), this kind of broad access is the definition of a SysAdmin.

HPSCI apparently never had a problem with techs getting direct access to our dragnet metadata, as they had and (now working in pairs) still have, for those of us two degrees away from a suspect.

Plus, HPSCI has never done anything publicly to help the 21 million clearance holders whose PII China now holds. Is it possible they're more angry at Snowden than they are at China's hackers, who have more ill-intent than Snowden?

But here's the other reason this complaint is laugh-out-loud funny. HPSCI closes its report this way:

> Finally, the Committee remains concerned that more than three years after the start of the unauthorized disclosures, NSA and the IC as a whole, have not done enough to minimize the risk of another massive unauthorized disclosure. Although it is impossible to reduce the change of another Snowden to zero, more work can and should be done to improve the security of the people and the computer networks that keep America's most closely held secrets. For instance, a recent DOD Inspector General report directed by the Committee had yet to effectively implement its post-Snowden security improvements. The Committee has taken actions to improve IC information security in the Intelligence Authorization Acts for Fiscal Years 2014, 2015, 2016, and 2017, and looks forward to working with the IC to continue to improve security.

First, that timeline — showing an effort to improve network security in each year following the Snowden leaks — is completely disingenuous. It neglects to mention that the Intel Committees

have actually been trying for longer than that. In the wake of the Manning leaks, it became clear that DOD's networks were sieve-like. Congress tried to require network monitoring in the 2012 Intelligence Authorization. But the Administration responded by insisting 2013 — 3 years after Manning's leaks — was too soon to plug all the holes in DOD's networks. One reason Snowden succeeded in downloading all those files is because the network monitoring hadn't been rolled out in Hawaii yet.

So HPSCI is trying to pretend Intel Committee past efforts didn't actually precede Snowden by several years, but those efforts failed to stop Snowden.

The other reason I find this paragraph — which appears just four paragraphs after it attacks Snowden for the invasion of his colleagues' privacy — so funny is that in the 2014 Intelligence Authorization (that is, the first one after the Snowden leaks), HPSCI codified an insider threat program, requiring the Director of National Intelligence to,

> ensure that the background of each employee or officer of an element of the intelligence community, each contractor to an element of the intelligence community, and each individual employee of such a contractor who has been determined to be eligible for access to classified information is monitored on a continual basis under standards developed by the Director, including with respect to the frequency of evaluation, during the period of eligibility of such employee or officer of an element of the intelligence community, such contractor, or such individual employee to such a contractor to determine whether such employee or officer of an element of the intelligence community, such contractor, and such individual employee of such a contractor continues to meet the

> requirements for eligibility for access to classified information;

This insider threat program searches IC employees hard drives (one of Snowden's sins).

Then, the following year, HPSCI got even more serious, mandating that the Director of National Intelligence look into credit reports, commercially available data, and social media accounts to hunt down insider threats, including by watching for changes in ideology like those Snowden exhibited, developing an outspoken concern about the Fourth Amendment.

I mean, on one hand, this isn't funny at all — and I imagine that Snowden's former colleagues blame him that they have gone from having almost no privacy as cleared employees to having none. This is what people like Carrie Cordero mean when they regret the loss of trust at the agency.

But as I have pointed out in the past, if someone like Snowden — who at least claims to have had good intentions — can walk away with the crown jewels, we should presume some much more malicious and/or greedy people have as well.

> But here's the thing: you cannot, as Cordero does, say that the "foreign intelligence collection activities [are] done with detailed oversight and lots of accountability" if it is, at the same time, possible for a SysAdmin to walk away with the family jewels, including raw data on targets. If Snowden could take all this data, then so can someone maliciously spying on Americans — it's just that that person wouldn't go to the press to report on it and so it can continue unabated. In fact, in addition to rolling out more whistleblower protections in the wake of Snowden, NSA has made some necessary changes (such as not permitting

> individual techs to have unaudited access to raw data anymore, which appears to have been used, at times, as a workaround for data access limits under FISA), even while ratcheting up the insider threat program that will, as Cordero suggested, chill certain useful activities. One might ask why the IC moved so quickly to insider threat programs rather than just implementing sound technical controls.

The Intelligence world has gotten itself into a pickle, at once demanding that a great deal of information be shared broadly, while trying to hide what information that includes, even from American citizens. It aspires to be at once an enormous fire hose and a leak-proof faucet. That is the inherent impossibility of letting the secret world grow so far beyond management — trying to make a fire hose leak proof.

Some people in the IC get that — I believe this is one of the reasons James Clapper has pushed to rein in classification, for example.

But HPSCI, the folks overseeing the fire hose? They don't appear to realize that they're trying to replicate and expand Snowden's privacy violations, even as they condemn them.