THE IC CAN'T EVEN DECIDE WHAT IS CLASSIFIED IN HILLARY'S EMAILS BUT THEY'RE ATTEMPTING TO DO SAME ON THE INTERNET

Yesterday, Steven Aftergood noted that, rather than prosecute leakers, the Intelligence Community is instead taking administrative measures against people who leak information. We've know they were moving in that direction for some time (largely through Aftergood's efforts). But he posts now de-classified testimony obtained via FOIA that Bob Litt gave in 2012 explaining the change.

> "This Administration has been historically active in pursuing prosecution of leakers, and the Intelligence Community fully supports this effort," said ODNI General Counsel Robert S. Litt in testimony from a closed hearing of the Senate Intelligence Committee in 2012 that was released last week in response to a Freedom of Information Act request.
>
> But, he said, "prosecution of unauthorized disclosure cases is often beset with complications, including difficult problems of identifying the leaker, the potential for confirming or revealing even more classified information in a public trial, and graymail by the defense."
>
> Therefore, Mr. Litt said, in 2011 Director of National Intelligence James Clapper ordered intelligence agencies "to pursue administrative investigations

> and sanctions against identified leakers wherever appropriate. Pursuant to this DNI directive, individual agencies are instructed to identify those leak incidents that are ripe for an administrative disposition….”

As Aftergood notes, such measures sure didn’t dissuade Edward Snowden.

There are two more interesting details of note in the testimony Aftergood liberated. First, Litt provides a somewhat redacted assessment of whether IC elements have the ability to audit employee activities on their networks. Most members of the IC has some audit and monitoring in place. Whereas some are what Litt describes as “robust,” he admitted that “other agencies have less mature programs, but some ability to track employee online activity.”

I do hope for Litt’s sake he didn’t tell SSCI, a year before Snowden’s leaks, that the NSA was among the agencies with robust systems, because they ended up having no ability to track what he took, much less see him taking huge amounts of data in real time.

Perhaps most interesting, though, is Litt’s reference to the development of “automated systems … that will assist in identifying classified information published on the Internet.” By Litt’s testimony on February 9, 2012, an IC study had “concluded that it would be beneficial and feasible for ONCIX/S to implement a centralized and automated capability to identify potential unauthorized disclosures of classified information published electronically on the Internet.” The IC was looking for funding to develop a pilot program to do just that in 2012.

The example of Hillary’s email is testament to one of many problems with such a plan. Various intelligence agencies accused her aides of sharing classified information. But in at least some cases, the same information was available

via open source (not to mention that it's easy to suss out what the IC thinks its biggest secrets are).

So the IC will be scanning the Internet for stuff they think is theirs. But short of tracking classification markings, this will necessarily involved scanning for either known leaked information (so imagine them currently tracking everyone discussing a document Snowden leaked, anywhere in the world), or scanning for information that looks to have the particular syntax (heh) of an intelligence report.

There are a range of problems I can imagine that would result.

But that likely won't stop the IC from trying to hold their glut of classified information inside their fences, or to hunt down people who seem to understand the same things the IC knows, in case that person can be caught talking to some person the IC would also like to enclose behind that fence.