WILL JAMES CLAPPER BE THE FIRST KNOWN VICTIM OF OMNICISA'S REGULATORY IMMUNITY?

According to Medium, Crackas With Attitude just hacked James Clapper and his wife.

> One of the group's hackers, who's known as "Cracka," contacted me on Monday, claiming to have broken into a series of accounts connected to Clapper, including his home telephone and internet, his personal email, and his wife's Yahoo email. While in control of Clapper's Verizon FiOS account, Cracka claimed to have changed the settings so that every call to his house number would get forwarded to the Free Palestine Movement.
>
> [snip]
>
> The hacker also sent me a list of call logs to Clapper's home number. In the log, there was a number listed as belonging to Vonna Heaton, an executive at Ball Aerospace and a former senior executive at the National Geospatial-Intelligence Agency. When I called that number, the woman who picked up identified as Vonna Heaton. When I told her who I was, she declined to answer any questions.

Viscerally, I'm laughing my ass off that Verizon (among others) has shared Clapper's metadata without his authority. "Not wittingly," they might say if he asks them about that. But I recognize that it's actually not a good thing for someone in such a sensitive position to have his metadata exposed (I mean, to the extent that

it wasn’t already exposed in the OPM hack).

I would also find some amusement if Clapper ends up being the first public victim of OmniCISA’s regulatory immunity for corporations.

Yahoo and Verizon can self-report this cyber intrusion to DHS, and if they do then the government can’t initiate regulatory action against them for giving inadequate protection from hacking for the Director of National Intelligence’s data.

And whether or not Clapper is the first victim of OmniCISA’s regulatory immunity, he is among the first Americans that the passage of OmniCISA failed to protect from hacking.