IN ONE OF HIS FIRST MAJOR LEGISLATIVE ACTS, PAUL RYAN TRYING TO DEPUTIZE COMCAST TO NARC YOU OUT TO THE FEDS

As the Hill reports, Speaker Paul Ryan is preparing to add a worsened version of the Cybersecurity Information Sharing Act to the omnibus budget bill, bypassing the jurisdictional interests of Homeland Security Chair Mike McCaul in order to push through the most privacy-invasive version of the bill.

> But several people tracking the negotiations believe McCaul is under significant pressure from House Speaker Paul Ryan (R-Wis.) and other congressional leaders to not oppose the compromise text.
>
> They said lawmakers are aiming to vote on the final cyber bill as part of an omnibus budget deal that is expected before the end of the year.

As I laid out in October, it appears CISA — even in the form that got voted out of the Senate — would serve as a domestic "upstream" spying authority, providing the government a way to spy

domestically without a warrant.

> CISA permits the telecoms to do the kinds of scans they currently do for foreign intelligence purposes for cybersecurity purposes in ways that (unlike the upstream 702 usage we know about) would not be required to have a foreign nexus. CISA permits the people currently scanning the backbone to continue to do so, only it can be turned over to and used by the government without consideration of whether the signature has a foreign tie or not. Unlike FISA, CISA permits the government to collect entirely domestic data.

We recently got an idea of how this might work. Comcast is basically hacking its own users to find out if they're downloading copyrighted material.

> [Comcast] has been accused of tapping into unencrypted browser sessions and displaying warnings that accuse the user of infringing copyrighted material — such as sharing movies or downloading from a file-sharing site.
>
> That could put users at risk, says the developer who discovered it.
>
> Jarred Sumner, a San Francisco, Calif.-based developer who published the alert banner's code on his GitHub page, told ZDNet in an email that this could cause major privacy problems.
>
> Sumner explained that Comcast injects the code into a user's browser as they are browsing the web, performing a so-called "man-in-the-middle" attack. (Comcast has been known to alert users when they have surpassed their data caps.) This means Comcast intercepts the traffic between a user's computer and their servers, instead of installing

> software on the user's computer.
>
> [snip]
>
> "This probably means that Comcast is using [deep packet inspection] on subscriber's internet and/or proxying subscriber internet when they want to send messages to subscribers," he said. "That would let Comcast modify unencrypted traffic in both directions."

In other words, Comcast is *already* doing the same kind of deep packet inspection of its users' unencrypted activity as the telecoms use in upstream collection for the NSA. Under CISA, they'd be permitted — and Comcast sure seems willing — to do such searches for the Feds.

Some methods of downloading copyrighted content might already be considered a cyberthreat indicator that Comcast could report directly to the Federal government (and possibly, under this latest version, directly to the FBI). And there are reports that the new version will adopt an expanded list of crimes, to include the Computer Fraud and Abuse Act.

In other words, it's really easy to see how under this version of CISA, the government would ask Comcast to *hack you* to find out if you're doing one of the long list of things considered hacking — a CFAA violation — by the Feds.

How's that for Paul Ryan's idea of conservatism, putting the government right inside your Internet router as one of his first major legislative acts?