COULD CORPORATIONS INCLUDE CISA NON-PARTICIPATION IN TRANSPARENCY REPORTS? WOULD IT EVEN MEAN ANYTHING?

I confess I don't know the answer to this question, but I'm going to pose it anyway. Could companies report non-participation in CISA — or whatever the voluntary cyber information sharing program that will soon roll out is eventually called — in their transparency reports?

I ask in part because there's great uncertainty about whether tech companies support or oppose the measure. The Business Software Alliance suggested they supported a data sharing bill, until Fight for the Future made a stink, when at least some of them pulled off (while a number of other BSA members, like Adobe, IBM, and Siemens, will surely embrace the bill). A number of companies have opposed CISA, either directly (like Apple) or via the Computer and Communications Industry Association. But even Google, which is a CCIA member, still wants a way to share information even if they express concerns about CISA's current form. Plus, there some indication that some of the companies claiming to oppose CISA — most notably, Facebook — are secretly lobbying in favor of it.

In the wake of CISA passing, activists are wondering if companies would agree not to participate (because participation is, as Richard Burr reminded over and over, voluntary, even if the key voluntary participants will also be bidding on a $50 billion contract as CISA rolls out). But I'm not sure what that would even mean.

So, first, would companies legally be permitted

to claim in their transparency reports that they did not voluntarily participate in CISA? There are a lot of measures that prohibit the involuntary release of information about companies' voluntary participation in CISA. But nothing in the bill that seems to prohibit the voluntary release of information about companies' voluntary non-participation.

But even if a company made such a claim — or claimed that they only share cyber indicators with legal process — would it even be meaningful? Consider: Most of the companies that might make such a claim get hacked. Even Apple, the company that has taken the lead on pushing back against the government, has faced a series of attacks and/or vulnerabilities of late, both in its code and its app store. Both any disclosures it made to the Federal government and to its app vendors would be covered by CISA unless Apple deliberately disclosed that information outside the terms of CISA — for example, by deliberately leaving personally identifiable information in any code it shared, which it's not about to do. Apple will enjoy the protections in CISA whether it asked for them or not. I can think of just two ways to avoid triggering the protections of CISA: either to only report such vulnerabilities as a crime report to FBI (which, because it bypassed the DHS, would not get full protection, and which would be inappropriate for most kinds of vulnerability disclosures), or to publicly disclose everything to the public. And that's assuming there aren't more specific disclosures — such as attempts to attack specific iCloud accounts — that would legitimately be intelligence reports. Google tells users if they think state actors are trying to compromise their accounts; is this appropriate to share with the government without process? Moreover, most of the companies that would voluntarily not participate already have people with clearance who can and do receive classified intelligence from the government. Plus, these companies can't choose not to let their own traffic that transits communications backbone be scanned by

the backbone owners.

In other words, I'm not sure how a company can claim not to participate in CISA once it goes into effect unless it doesn't share any information. And most of the big tech companies are already sharing this information among themselves, they want to continue to do that sharing, and that sharing would get CISA protections.

The problem is, there are a number of kinds of information sharing that will get the permission of CISA, all of which would count as "participating in it." Anything Apple shared with the government or other companies would get CISA protection. But that's far different than taking a signature the government shares and scanning all backbone traffic for instances of it, which is what Verizon and AT&T will almost certainly be doing under CISA. That is, there are activities that shouldn't require legal process, and activities that currently do but will not under CISA. And to get a meaningful sense of whether someone is "participating" in CISA by performing activities that otherwise would require legal process, you'd need a whole lot of details about what they were doing, details that not even criminal defendants will ever get. You'd even need to distinguish activities companies would do on their own accord (Apple's own scans of its systems for known vulnerabilities) from things that came pursuant to information received from the federal government (a scan on a vulnerability Apple learned about from the government).

We're never going to get that kind of information from a transparency report, except insofar as companies detail the kinds of things they require legal process for in spite of CISA protection for doing them without legal process. That would not be the same thing as non-participation in CISA — because, again, most of the companies that have raised objections already share information at least with industry partners. But that's about all we'd get short of

really detailed descriptions of any scrubbing that goes on during such information sharing.