LEGAL ANALYSIS OF OMNICISA REINFORCES CAUSE FOR CONCERN

Among all the commentaries about CISA published before its passage, only one I know of (aside from my non-lawyer take here) dealt with what the bill did legally: this Jennifer Granick post explaining how OmniCISA will "stake out a category of ISP monitoring that the FCC and FTC can't touch, regardless of its privacy impact on Americans," thereby undercutting recent efforts to increase online privacy.

Since the bill passed into law, however, two lawyers have written really helpful detailed posts on what it does: Fourth Amendment scholar Orin Kerr and former NSA lawyer Susan Hennessey.

As Kerr explains, existing law had permitted Internet operators to surveil their own networks for narrowly tailored upkeep and intrusion purposes. OmniCISA broadened that to permit a provider to monitor (or have a third party monitor) both the network and traffic for a cybersecurity purpose.

> [T]he right to monitor appears to extend to "cybersecurity purposes" generally, not just for the protection of the network operator's own interests. And relatedly, the right to monitor includes scanning and acquiring data that is merely transiting the system, which means that the network operator can monitor (or have someone else monitor) for cybersecurity purposes even if the operator isn't worried about his own part of the network being the victim. Note the difference between this and the provider exception. The provider exception is about protecting the provider's own network. If I'm reading the language here correctly, this is a

> broader legal privilege to monitor for cybersecurity threats.

It also permits such monitoring for insider threats.

> [T]he Cyber Act may give network operators broad monitoring powers on their own networks to catch not only hackers but also insiders trying to take information from the network.

This accords with Hennessey's take (and of course, having recently worked at NSA, she knows what they were trying to do). Importantly, she claims providers need to surveil *content* to take "responsible cybersecurity measures."

> Effective cybersecurity includes network monitoring, scanning, and deep-packet inspection—and yes, that includes contents of communications—in order to detect malicious activity.

In spite of the fact that Hennessey explicitly responded to Granick's post, and Granick linked a letter from security experts describing the limits of what was really necessary for monitoring networks, Hennessey doesn't engage in those terms to explain why corporations need to spy on their customers' content to take responsible cybersecurity measures. It may be as simple as needing to search the contents of packets for known hackers' signatures, or it may relate to surveilling IP theft or it may extend to reading the content of emails; those are fairly different degrees of electronic surveillance, all of which might be permitted by this law. But credit Hennessey for making clear what CISA boosters in Congress tried so assiduously to hide: this is about warrantless surveillance of *content*.

Hennessey lays out why corporations need a new law to permit them to spy on their users' content, suggesting they used to rely on user

agreements to obtain permission, but pointing to several recent court decisions that found user agreements did not amount to implied consent for such monitoring.

> If either party to a communication consents to its interception, there is no violation under ECPA, "unless such communication is intercepted for the purpose of committing any criminal or tortious act." 18 USC 2511(2)(d). Consent may be express or implied but, in essence, authorized users must be made aware of and manifest agreement to the interception.
>
> At first glance, obtaining effective consent from authorized users presents a simple and attractive avenue for companies and cyber security providers to conduct monitoring without violating ECPA. User agreements can incorporate notification that communications may be monitored for purposes of network security. However, the ambiguities of ECPA have resulted in real and perceived limitations on the ability to obtain legally-effective consent.
>
> Rapidly evolving case law generates significant uncertainty regarding the scope of consent as it relates to electronic communications monitoring conducted by service providers. In Campbell v. Facebook, a court for the Northern District of California denied Facebook's motion to dismiss charges under ECPA, rejecting the claim that Facebook had obtained user consent. Despite lengthy user agreements included in Facebook's "Statement of Rights and Responsibilities" and "Data Use Policy," the court determined that consent obtained "with respect to the processing and sending of messages does not necessarily constitute consent to … the scanning of message content for use in

> targeted advertising." Likewise in ln re Google Inc. Gmail Litigation, the same district determined that Google did not obtain adequate consent for the scanning of emails, though in that case, Google's conduct fell within the "ordinary course of business" definition and thus did not constitute interception for the purposes of ECPA.
>
> Here, and in other instances, courts have determined that companies which are highly sophisticated actors in the field have failed to meet the bar for effective consent despite good faith efforts to comply.

Hennssey's focus on cases affecting Facebook and, especially, Google provide a pretty clear idea why those and other tech companies were pretending to oppose CISA without effectively doing so (Google's Eric Schmidt had said such a law was necessary, but he wasn't sure if this law was what was needed).

Hennessey goes on to extend these concerns to third party permission (that is, contractors who might monitor another company's network, which Kerr also noted). Perhaps most telling is her discussion of those who don't count as electronic communications service providers.

> Importantly, a large number of private entities require network security monitoring but are not themselves electronic communication service providers. For those entities that do qualify as service providers, it is not unlawful to monitor communications while engaged in activity that is a "necessary incident to" the provision of service or in order to protect the "rights or property" of the provider. But this exception is narrowly construed. In general, it permits providers the right "to intercept and monitor [communications] placed over their

> facilities in order to combat fraud and theft of service." U.S. v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). In practice, the exception does not allow for unlimited or widespread monitoring nor does it, standing alone, expressly permit the provision of data collected under this authority to the government or third parties.

Note how she assumes non-ECSPs would need to conduct "unlimited" monitoring and sharing with the government and third parties. That goes far beyond her claims about "responsible cybersecurity measures," without any discussion of how such unlimited monitoring protects privacy (which is her larger claim).

Curiously, Hennessey entirely ignores what Kerr examines (and finds less dangerous than tech companies' statements indicated): counter–er, um, defensive measures, which tech companies had worried would damage their infrastructure. As I noted, Richard Burr went out of his way to prevent Congress from getting reporting on whether that happened, which suggests it's a real concern. Hennessey also ignores something that totally undermines her claim this is about "responsible cybersecurity measures" – the regulatory immunity that guts the tools the federal government currently uses to require corporations to take such measures. She also doesn't explain why OmniCISA couldn't have been done with the same kind of protections envisioned for "domestic security" surveillance under *Keith* and FISA, which is clearly what CISA is: notably, court review (I have suggested it is likely that FISC refused to permit this kind of surveillance).

I am grateful for Hennessey's candor in laying out the details that a functional democracy would have laid out before eliminating the warrant requirement for some kinds of domestic wiretapping.

But it's also worth noting that, even if you

concede that permitting corporations such unfettered monitoring of their customers, even if you assume that the related info-sharing is anywhere near the most urgent thing we can do to prevent network intrusions, OmniCISA does far more than what Hennessey lays out as necessary, much of which is designed to shield all this spying, and the corporations that take part in it, from real review.

Hennessey ends her post by suggesting those of us who are concerned about OmniCISA's broad language are ignoring limitations within it.

> Despite vague allegations from critics that "cybersecurity purpose" could be read to be all-encompassing, the various definitions and limitations within the act work to create a limited set of permissible activities.

But even if that were true, it'd be meaningless given a set-up that would subject this surveillance only to Inspectors General whose past very diligent efforts to fix abuses have failed. *Not even Congress* will get key information — such as how often this surveillance leads to a criminal investigation or how many times "defensive measures" break the Internet — it needs to enforce what few limitations there are in this scheme.

All of which is to say that people with far more expertise than I have are reviewing this law, and their reviews only serve to confirm my earlier concerns.