HOW THE PURPOSE OF THE DATA SHARING PORTAL CHANGED OVER THE OMNICISA DEBATE

Last year, House Homeland Security Chair Michael McCaul offered up his rear-end to be handed back to him in negotiations leading to the passage of OmniCISA on last year's omnibus. McCaul was probably the only person who could have objected to such a legislative approach because it deprived him of weighing in as a conferee. While he made noise about doing so, ultimately he capitulated and let the bill go through — and be made less privacy protective — as part of the must-pass budget bill.

Which is why I was so amused by McCaul's op-ed last week, including passage of OmniCISA among the things he has done to make the country more safe from hacks. Here was a guy, holding his rear-end in his hands, plaintively denying that, by claiming that OmniCISA reinforced his turf.

> I was adamant that the recently-enacted Cybersecurity Act include key provisions of my legislation H.R. 1731, the National Cybersecurity Protection Advancement Act. With this law, we now have the ability to be more efficient while protecting both our nation's public and private networks.
>
> With these new cybersecurity authorities signed into law, the Department of Homeland Security (DHS) will become the sole portal for companies to voluntarily share information with the federal government, while preventing the military and NSA from taking on this role in the future.
>
> With this strengthened information-sharing portal, it is critical that we provide incentives to private

> companies who voluntarily share known cyber threat indicators with DHS. This is why we included liability protections in the new law to ensure all participants are shielded from the reality of unfounded litigation.
>
> While security is vital, privacy must always be a guiding principle. Before companies can share information with the government, the law requires them to review the information and remove any personally identifiable information (PII) unrelated to cyber threats. Furthermore, the law tasks DHS and the Department of Justice (DOJ) to jointly develop the privacy procedures, which will be informed by the robust existing DHS privacy protocols for information sharing.
>
> [snip]
>
> Given DHS' clearly defined lead role for cyber information sharing in the Cybersecurity Act of 2015, my Committee and others will hold regular oversight hearings to make certain there is effective implementation of these authorities and to ensure American's privacy and civil liberties are properly protected.

It is true that under OmniCISA, DHS is currently (that is, on February 1) the sole portal for cyber-sharing. It's also true that OmniCISA added DHS, along with DOJ, to those in charge of developing privacy protocols. There are also other network defense measures OmniCISA tasked DHS with — though the move of the clearances function, along with the budget OPM had been asking for to do it right but not getting, to DOD earlier in January, the government has apparently adopted a preference for moving its sensitive functions to networks DOD (that is, NSA) will guard rather than DHS. But McCaul's bold claims really make me wonder about the

bureaucratic battles that may well be going on as we speak.

Here's how I view what actually happened with the passage of OmniCISA. It is heavily influenced by these three Susan Hennessey posts, in which she tried to convince that DHS' previously existing portal ensured privacy would be protected, but by the end seemed to concede that's not how it might work out.

1. CISA in Context: Privacy Protections and the Portal
2. CISA in Context: The Voluntary Sharing Model and that "Other" Portal
3. CISA in Context: Government Use and What Really Matters for Civil Liberties

Underlying the entire OmniCISA passage is a question: Why was it necessary? Boosters explained that corporations wouldn't share willingly without all kinds of immunities, which is surely true, but the same boosters never explained why an info-sharing system was so important when experts were saying it was way down the list of things that could make us safer and similar info-sharing has proven not to be a silver bullet. Similarly, boosters did not explain the value of a system that not only did nothing to require cyber information shared with corporations would be used to protect their networks, but by giving them immunity (in final passage) if they did nothing with information and then got pawned, made it less likely they will use the data. Finally, boosters ignored the ways in which OmniCISA not only creates privacy risks, but also expands new potential vectors of attack or counterintelligence collection for our adversaries.

So why was it necessary, especially given the many obvious ways in which it was not optimally designed to encourage monitoring, sharing, *and implementation* from network owners? Why was it necessary, aside from the fact that our Congress

has become completely unable to demand corporations do anything in the national interest and there was urgency to pass something, anything, no matter how stinky?

Indeed, why was legislation doing anything except creating some but not all these immunities necessary if, as former NSA lawyer Hennessey claimed, the portal laid out in OmniCISA in fact got up and running on October 31, between the time CISA passed the Senate and the time it got weakened significantly and rammed through Congress on December 18?

> At long last DHS has publically unveiled its new CISA-sanctioned, civil-liberties-intruding, all-your-personal-data-grabbing, information-sharing uber vacuum. Well, actually, it did so three months ago, right around the time these commentators were speculating about what the system would look like. Yet even as the cleverly-labeled OmniCISA passed into law last month, virtually none of the subsequent commentary took account of the small but important fact that the DHS information sharing portal has been up and running for months.

Hennessey appeared to think this argument was very clever, to suggest that "virtually no" privacy advocates (throughout her series she ignored that opposition came from privacy *and* security advocates) had talked about DHS' existing portal. She must not have Googled that claim, because if she had, it would have become clear that privacy (and security) people had discussed DHS' portal back in August, before the Senate finalized CISA.

Back in July, Al Franken took the comedic step of sending a letter to DHS basically asking, "Say, you're already running the portal that is being legislated in CISA. What do you think of the legislation in its current form?" And DHS wrote back and noted that the portal being laid out in CISA (and the other sharing permitted

under the bill) *was different in several key* ways from what it was already implementing.

Its concerns included:

- *Because companies could share with other agencies, the bill permitted sharing* ***content*** *with law enforcement.* "The authorization to share cyber threat indicators and defensive measures with 'any other entity or the Federal Government,' 'notwithstandin g any other provision of law' could sweep away important privacy protections, particularly the provisions in the Stored Communications Act limiting the disclosure of the content of electronic communications to the government by certain providers."
- *The bill permitted companies to share more information than that permitted under the existing portal*. "Unlike the President's proposal, the Senate bill includes 'any other attribute of a cybersecurity threat' within its definition of cyber threat indicator."
- *Because the bill required sharing in real time rather*

than in near-real time, it would mean DHS could not do all the privacy scrubs it was currently doing. "If DHS distributes information that is not scrubbed for privacy concerns, DHS would fail to mitigate and in fact would contribute to the compromise of personally identifiable information by spreading it further."

- *Sharing in real rather than near-real time also means participants might get overloaded with extraneous information (something that has made existing info-sharing regimes ineffective)*. "If there is no layer of screening for accuracy, DHS' customers may receive large amounts of information with dubious value, and may not have the capability to meaningfully digest that information."
- *The bill put the Attorney General, not DHS, in charge of setting the rules for the portal.* "Since sharing cyber threat information with the private sector is primarily within DHS's mission space, DHS should author the section 3 procedures, in coordination with other

entities."

- *The 90-day implementation timeline was too ambitious; according to DHS, the bill should provide for an 180-day implementation*. "The 90-day timeline for DHS's deployment of a process and capability to receive cyber threat indicators is too ambitious, in light of the need to fully evaluate the requirements pertaining to that capability once legislation passes and build and deploy the technology."

As noted, that exchange took place in July (most responses to it appeared in August). While a number of amendments addressing DHS' concerns were proposed in the Senate, I'm aware of only two that got integrated into the bill that passed: an Einstein (that is, federal network monitoring) related request, and DHS got added — along with the Attorney General — in the rules-making function. McCaul mentioned both of those things, along with hailing the "more efficient" sharing that may refer to the real-time versus almost real-time sharing, in his op-ed.

Not only didn't the Senate respond to most of the concerns DHS raised, as I noted in another post on the portal, the Senate also gave other agencies veto power over DHS' scrub (this was sort of the quid pro quo of including DHS in the rule-making process, and it was how Ranking Member on the Senate Homeland Security Committee, Tom Carper, got co-opted on the bill), which exacerbated the real versus almost real-time sharing problem.

All that happened by October 27, days before the portal based on Obama's executive order got

fully rolled out. The Senate literally passed changes to the portal as DHS was running it days before it went into full operation.

Meanwhile, one more thing happened: as mandated by the Executive Order underlying the DHS portal, the Privacy and Civil Liberties Oversight Board helped DHS set up its privacy measures. This is, as I understand it, the report Hennessey points to in pointing to all the privacy protections that will make OmniCISA's elimination of warrant requirements safe.

> Helpfully, DHS has released its Privacy Impact Assessment of the AIS portal which provides important technical and structural context. To summarize, the AIS portal ingests and disseminates indicators using—acronym alert!—the Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). Generally speaking, STIX is a standardized language for reporting threat information and TAXII is a standardized method of communicating that information. The technology has many interesting elements worth exploring, but the critical point for legal and privacy analysis is that by setting the STIX TAXII fields in the portal, DHS controls exactly which information can be submitted to the government. If an entity attempts to share information not within the designated portal fields, the data is automatically deleted before reaching DHS.

In other words, the scenario is precisely the reverse of what Hennessey describes: DHS set up a portal, and then the Senate tried to change it in many ways that DHS said, *before passage*, would weaken the privacy protections in place.

Now, Hennessey does acknowledge some of the ways OmniCISA weakened privacy provisions that were

in DHS' portal. She notes, for example, that the Senate added a veto on DHS' privacy scrubs, but suggests that, because DHS controls the technical parameters, it will be able to overcome this veto.

> At first read, this language would appear to give other federal agencies, including DOD and ODNI, veto power over any privacy protections DHS is unable to automate in real-time. That may be true, but under the statute and in practice DHS controls AIS; specifically, it sets the STIX TAXXI fields. Therefore, DHS holds the ultimate trump card because if that agency believes additional privacy protections that delay real-time receipt are required and is unable to convince fellow federal entities, then DHS is empowered to simply refuse to take in the information in the first place. This operates as a rather elegant check and balance system. DHS cannot arbitrarily impose delays, because it must obtain the consent of other agencies, if other agencies are not reasonable DHS can cut off the information, but DHS must be judicious in exercising that option because it also loses the value of the data in question.

This seems to flip Youngstown on its head, suggesting the characteristics of the portal laid out in an executive order *and changed in legislation* take precedence over the legislation.

Moreover, while Hennessey does discuss the threat of the other portal — one of the features added in the OmniCISA round with no debate — she puts it in a different post from her discussion of DHS' purported control over technical intake data (and somehow portrays it as having "emerged from conference with the new possibility of an alternative portal" even though no actual conference took place, which is why McCaul is stuck writing plaintive op-eds while holding his

rear-end). This means that, after writing a post talking about how DHS would have the final say on protecting privacy by controlling intake, Hennessey wrote another post that suggested DHS would have to "get it right" or the President would order up a second portal without all the privacy protections that DHS' portal had in the first place (and which it had already said would be weakened by CISA).

> Such a portal would, of course, be subject to all statutory limitations and obligations, including codified privacy protections. But the devil is in the details here; specifically, the details coded into the sharing portal itself. CISA does not obligate that the technical specifications for a future portal be as protective as AIS. This means that it is not just the federal government and private companies who have a stake in DHS getting it right, but privacy advocates as well. The balance of CISA is indeed delicate.

Elsewhere, Hennessey admits that many in government think DHS is a basket-case agency (an opinion I'm not necessarily in disagreement with). So it's unclear how DHS would retain any leverage over the veto given that exercising such leverage would result in DHS losing this portfolio altogether. There was a portal designed with privacy protections, CISA undermined those protections, and then OmniCISA created yet more bureaucratic leverage that would force DHS to eliminate its privacy protections to keep the overall portfolio.

Plus, OmniCISA did two more things. First, as noted, back in July DHS said it would need 180 days to fully tweak its existing portal to match the one ordered up in CISA. CISA and OmniCISA didn't care: the bill and the law retained the 90 day turnaround. But in addition, OmniCISA required DHS and the Attorney General develop their interim set of guidelines within 60 days (which as it happened included the Christmas

holiday). That 60 deadline is around February 16. The President can't declare the need for a second portal until after the DHS one gets certified, which has a 90 day deadline (so March 18). But he can give a 30 day notice that's going to happen beforehand. In other words, the President can determine, after seeing what DHS and AG Lynch come up with in a few weeks, that that's going to be too privacy restrictive and tell Congress FBI needs to have its own portal, something that did not and would not have passed under regular legislative order.

Finally, as I noted, PCLOB had been involved in setting up the privacy parameters for DHS' portal, including the report that Hennessey points to as the basis for comfort about OmniCISA's privacy risk. In final passage of OmniCISA, a PCLOB review of the privacy impact of OmniCISA, which had been included in every single version of the bill, got eliminated.

Hennssey's seeming admission that's the eventual likelihood appears over the course of her posts as well. In her first post, she claims,

> From a practical standpoint, the government does not want any information—PII or otherwise—that is not necessary to describe or identify a threat. Such information is operationally useless and costly to store and properly handle.

But in explaining the reason for a second portal, she notes that there is (at least) one agency included in OmniCISA sharing that does want more information: FBI.

> [T]here are those who fear that awarding liability protection exclusively to sharing through DHS might result in the FBI not getting information critical to the investigation of computer crimes. The merits of the argument are contested but the overall intention of CISA is certainly not to result in the FBI

> getting less cyber threat information. Hence, the fix.
>
> [snip]
>
> AIS is not configured to receive the full scope of cyber threat information that might be necessary to the investigation of a crime. And while CISA expressly permits sharing with law enforcement — consistent with all applicable laws — for the purposes of opening an investigation, the worry here is that companies that are the victims of hacks will share those threat indicators accepted by AIS, but not undertake additional efforts to lawfully share threat information with an FBI field office in order to actually investigate the crime.

That is, having decided that the existing portal wasn't good enough because it didn't offer enough immunities (and because it was too privacy protective), the handful of mostly Republican leaders negotiating OmniCISA outside of normal debate then created the possibility of extending those protections to a completely different kind of information sharing, that of content shared for law enforcement.

In her final post, Hennessey suggests some commentators (hi!!) who might be concerned about FBI's ability to offer immunity for those who share domestically collected content willingly are "conspiracy-minded" even while she reverts to offering solace in the DHS portal protections that, her series demonstrates, are at great risk of bureaucratic bypass.

> But these laws encompass a broad range of computer crimes, fraud, and economic espionage — most controversially the Computer Fraud and Abuse Act (CFAA). Here the technical constraints of the AIS system cut both ways. On one hand, the scope of cyber threat indicators

> shared through the portal significantly undercuts claims CISA is a mass surveillance bill. Bluntly stated, the information at issue is not of all that much use for the purposes certain privacy-minded — and conspiracy-minded, for that matter — critics allege. Still, the government presumably anticipates using this information in at least some investigations and prosecutions. And not only does CISA seek to move more information to the government — a specific and limited type of information, but more nonetheless — but it also authorizes at least some amount of new sharing.
>
> [snip]
>
> That question ultimately resolves to which STIX TAXII fields DHS decides to open or shut in the portal. So as CISA moves towards implementation, the portal fields — and the privacy interests at stake in the actual information being shared — are where civil liberties talk should start.

To some degree, Hennessey's ultimate conclusion is one area where privacy (and security) advocates might weigh in. When the government provides Congress the interim guidelines sometime this month, privacy (and security) advocates might have an opportunity to weigh in, if they get a copy of the guidelines. But only the final guidelines are required to be made public.

And by then, it would be too late. Through a series of legislative tactics, some involving actual debate but some of the most important simply slapped onto a must-pass legislation, Congress has authorized the President to let the FBI, effectively, obtain US person content pertaining to Internet-based crimes without a warrant. Even if President Obama chooses not to use that authorization (or obtains enough

concessions from DHS not to have to directly), President Trump may not exercise that discretion.

Maybe I am being conspiratorial in watching the legislative changes made to a bill (and to an existing portal) and, absent any other logical explanation for them, concluding those changes are designed to do what they look like they're designed to do. But it turns out privacy (and security) advocates weren't conspiratorial enough to prevent this from happening before it was too late.