

Dear Colleague,

I am writing to express my concerns with the inclusion of the Cybersecurity Act in the omnibus. What was intended to be a cybersecurity bill to facilitate the sharing of information between the private sector and government was instead drafted in such a way that it has effectively become a surveillance bill, and allows information shared by companies to be used by the government to prosecute unrelated crimes.

The bill intended to allow the private sector to share “cyber threat indicators” with government agencies. However, depending on the type of “indicator,” it is highly likely that private information otherwise protected by the Fourth Amendment will also be disclosed to government surveillance agencies.

Unfortunately, as drafted, the bill falls short of providing safeguards to protect Americans private information.

In particular:

1. This bill allows the use of shared information for more than just “cybersecurity purposes.” It allows the government to investigate and prosecute specific threats to serious bodily injury or serious economic injury, computer fraud, and trade secrets violations, among other criminal violations.

**WHY THIS IS OF CONCERN: Specific threats to serious bodily injury or economic harm are extremely broad categories of crimes. So are identity theft, computer fraud, and trade secrets violations. By allowing the use of this information for non-cybersecurity purposes, the bill encourages intelligence agencies to collect and retain as much information as they can for as long as possible, in the unlikely event that one day it might be useful. An alternative bill, H.R. 1731, which received the largest House support, prohibited these uses and limited the use of cyber indicators to only cyber security purposes for this reason.**

2. The bill fails to include an express prohibition on using this information for “surveillance” purposes.

**WHY THIS IS OF CONCERN: Express prohibition of “surveillance” is vital because past experience demonstrates that intelligence agencies will broadly interpret the included non-cyber, criminal allowances to perform surveillance. For example, few thought the National Security Agency (NSA) would interpret “relevant” to allow collection of every phone record in America. Surveillance is merely an investigation method, so this bill contains no protections against the NSA (or any other agency) from**

**conducting broad surveillance using this information in the name of stopping any enumerated offenses.**

3. The private sector and government are only required to remove personal information they “know at the time of sharing” to be included in the information they share with DHS.

**WHY THIS IS OF CONCERN:** The information sharing legislation that passed the House with the strongest support, H.R. 1731, required both government and private sector to take “*reasonable efforts*” to scrub all personal information “*reasonably believed*” to be unrelated to a cybersecurity threat prior to sharing the information. Changing this to a “knowing” standard, as the Cybersecurity Act does, sets the bar too high. Developing automated systems to “*know*” that something is personal information is likely impossible. As such, the “*knowing*” standard encourages willful blindness. Why would the government or private sector expend time and effort to develop effective processes to determine when it “knows” something is personal information rather than just develop a  cursory review process likely to permit the flow of private personal information.

Furthermore, by limiting scrubbing only to “the time of sharing” there is no requirement that the government remove personal information it later discovers. Finally, the bill leaves details on how to develop privacy protection procedures around the collection, storage, and retention of shared information to DHS and also to the Attorney General and Director of National Intelligence. The AG and DNI also determined these same standards for the bulk-collection of telephone metadata. These standards allowed for the largest abuse of American privacy in recent history and necessitated Congress passing the USA FREEDOM Act.

4. No express limitations on what or how DHS can share information with the DOD or NSA

**WHY THIS OF CONCERN:** Earlier this year Congress passed major privacy reforms because past experience has shown that if the NSA acquires information, they will use it in ways unintended by legislators. Every cybersecurity bill passed by the House this year has prohibited automatic information sharing (and in some cases all sharing) with the NSA. Without this prohibition, designating DHS as the “sole information sharing portal” is essentially meaningless, since DOD and NSA automatically receive cyber threat indicators along with the rest of civilian agencies. As this bill is drafted, functionally—there is no difference between directly giving this information to DHS and directly giving it to the NSA. There should be strong rules protecting personal

**information from being received, processed, and stored by intelligence agencies, which this bill lacks.**