GM SUPPORTS OBTAINING CYBERSECURITY IMMUNITY JUST AFTER HACK VULNERABILITY REVEALED

Dianne Feinstein just gave a long speech on the Senate floor supporting the Cyber Information Sharing Act.

She listed off a list of shocking hacks that happened in the last year or so – though made no effort (or even claim) that CISA would have prevented any of them.

She listed some of the 56 corporations and business organizations that support the bill.

Most interestingly, she boasted that yesterday she received a letter from GM supporting the bill. We should pass CISA, Feinstein suggests, because General Motors, on August 4, 2015, decided to support the bill.

I actually think that's reason to oppose the bill.

As I have written elsewhere – most recently this column at the DailyDot – one of my concerns about the bill is the possibility that by sharing data under the immunity afforded by the bill, corporations might dodge liability where it otherwise might serve as necessary safety and security leverage.

> Immunizing corporations may make it harder for the government to push companies to improve their security. As Wyden explained, while the bill would let the government use data shared to prosecute crimes, the government couldn't use it to demand security improvements at those companies. "The

> bill creates what I consider to be a double standard—really a bizarre double standard in that private information that is shared about individuals can be used for a variety of non-cyber security purposes, including law enforcement action against these individuals," Wyden said, "but information about the companies supplying that information generally may not be used to police those companies."
>
> Financial information-sharing laws may illustrate why Wyden is concerned. Under that model, banks and other financial institutions are obligated to report suspicious transactions to the Treasury Department, but, as in CISA, they receive in return immunity from civil suits as well as consideration in case of sanctions, for self-reporting. "Consideration," meaning that enforcement authorities take into account a financial institution's cooperation with the legally mandated disclosures when considering whether to sanction them for any revealed wrongdoing. Perhaps as a result, in spite of abundant evidence that banks have facilitated crimes—such as money laundering for drug cartels and terrorists—the Department of Justice has not managed to prosecute them. When asked during her confirmation hearing why she had not prosecuted HSBC for facilitating money laundering when she presided over an investigation of the company as U.S. Attorney for the Eastern District of New York, Attorney General Loretta Lynch said there was not sufficient "admissible" evidence to indict, suggesting they had information they could not use.

In the same column, I pointed out the different approach to cybersecurity – for cars

at least – of the SPY Act – introduced by Ed Markey and Richard Blumenthal – which affirmatively requires certain cybersecurity *and privacy* protections.

> Increased attention on the susceptibility of networked cars—heightened by but not actually precipitated by the report of a successful remote hack of a Jeep Cherokee—led two other senators, Ed Markey and Richard Blumenthal, to adopt a different approach. They introduced the Security and Privacy in Your Car Act, which would require privacy disclosures, adequate cybersecurity defenses, and additional reporting from companies making networked cars and also require that customers be allowed to opt out of letting the companies collect data from their cars.
>
> The SPY Car Act adopts a radically different approach to cybersecurity than CISA in that it requires basic defenses from corporations selling networked products. Whereas CISA supersedes privacy protections for consumers like the Electronic Communications Privacy Act, the SPY Car Act would enhance privacy for those using networked cars. Additionally, while CISA gives corporations immunity so long as they share information, SPY Car emphasizes corporate liability and regulatory compliance.

I'm actually not sure how you could have both CISA and SPY Act, because the former's immunity would undercut the regulatory limits on the latter. (And I asked both Markey and Blumenthal's offices, but they blew off repeated requests for an answer on this point.)

Which brings me back to GM's decision – yesterday!!! – to support CISA.

The hackers that remotely hacked a car used a Jeep Cherokee. But analysis they did last year found the Cadillac Escalade to be the second most hackable car among those they reviewed (and I have reason to believe there are other GM products that are probably even more hackable).

So … hackers reveal they can remotely hack cars on July 21; Markey introduced his bill on the same day. And then on August 4, GM for the first time signs up for a bill that would give them immunity if they start sharing data with the government in the name of cybersecurity.

Now maybe I'm wrong in my suspicion that CISA's immunity would provide corporations a way to limit their other liability for cybersecurity so long as they had handed over a bunch of data to the government, even if it incriminated them.

But we sure ought to answer that question before we go immunizing corporations whose negligence might leave us more open to attack.