Congress should pass the 'Fourth Amendment Is Not For Sale Act'

We've all watched the cringeworthy hearings where senators take turns "grilling" Big Tech CEOs over why their constituent emails have such low open rates. While the fight over regulating Big Tech rages, Americans' 4th Amendment rights continue to be abused in other areas that *do* in fact require a measured response. As it turns out, such a remedy already exists.

Last April, a group of bipartisan senators introduced The

Fourth Amendment Is Not For Sale Act (FANFSA).

In the Senate, the bill enjoys 20 co-sponsors ranging from Sens. Rand Paul (R-Ky.) to Bernie Sanders (I-VT). While the House companion bill is sponsored by Judiciary Chairman Jerrold Nadler (D-N.Y.), the bill has yet to see the light of day. That must change.

The Fourth Amendment protects the right to be free from unreasonable searches and seizures, unless the government acts with a judicially granted warrant supported by probable cause or there is an applicable exception to the warrant. The Supreme Court has recognized

that the Fourth Amendment provides protection from government searches when a person has a subjective expectation of privacy that society recognizes as objectively reasonable. See Katz v United States (1967) (Harlan, J., concurring). However, the Court has also held that a person does not have a legitimate expectation of privacy in information knowingly shared with third parties. See Smith v Maryland (1979).

The Court chipped away at this so-called "third party doctrine" in Carpenter

v United States (2018). The issue in Carpenter was whether there was a legitimate expectation of privacy in cell-site location information (CSLI). A CSLI is created every time a phone connects to a cell site, often found on a tower. Wireless providers store this information. The FBI sought CSLIs from wireless providers to find out how close Carpenter was to a string of robberies. Even though CSLIs are held by third parties, the Court held there was legitimate expectation of privacy. However, the Court noted that its holding was "narrow."

Congress has passed several statutes to combat the third-party doctrine that provide protection when the government seeks your information from internet, wireless, social media, or email providers. Under the Stored Communications Act (SCA) passed in 1986, these providers

are among a class of providers considered electronic communication services (ECS) or remote computing services (RCS). Most importantly, this means the government needs some form of court approval to access your content from a provider. For example, when a subpoena required Facebook to disclose private messages, a federal court quashed the subpoena because it did not comply with the stringent standards of the SCA. See Crispin v. Christian Audigier, *Inc*. (C.D. Cal. 2010).

At 36 years old, the SCA needs an update. The SCA does not protect consumers from data brokers that collect consumer information from common apps or websites. Because these data brokers do not provide the ability to send or receive the content at issue, they do not fall within the reach of the SCA. Therefore, if the government wants your information, they need no court approval. As a result, data brokers like Venntel can collect location data from smartphones and sell it to government agencies. Or even worse, data broker Clearview AI can create a massive database of photos from Facebook, LinkedIn, and Twitter and sell it to government agencies.

FANSFA would amend the SCA to treat data brokers just like it treats an ECS or RCS. In other words, the same court approval standards that apply when the government wants your personal messages from Facebook or Twitter will now apply when the government wants your information from Venntel, Clearview AI, or any other data broker. The statute explicitly prohibits the government from getting access to your information held by data brokers unless SCA processes are followed. Moreover, the bill prohibits the government from purchasing your information from data brokers.

There are other important structural reforms, too. In the event the government does illegally obtain your data, it cannot be used as evidence elsewhere like a court or legislative body. FANFSA also prohibits the attorney general from offering civil immunity to providers

- **Voters split on whether Senate should require supermajority to pass...**
- **Biden calls for changing Senate rules to allow voting bills to pass**

that assist the government in illegal surveillance. Importantly, providers retain immunity if surveillance assistance is ordered by a court.

Because of the everyday advancements in our technological world, Congress often fails to keep up. FANSFA is a rare exception. This legislation requires the government to go through the same court approval process as if it sought your personal messages from Facebook or Twitter. Your information is important. The government should not be able to buy it from data brokers because you decided to browse the internet. Congress must reignite the fight to protect the privacy of all Americans and pass FANSFA to correct this loophole.