July 20, 2021

The Honorable Dick Durbin
Chair
152 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Chuck Grassley
Ranking Member
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Jerry Nadler
Chair
2138 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jim Jordan
Ranking Member
2142 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Durbin, Ranking Member Grassley, Chairman Nadler, and Ranking Member Jordan:

The undersigned organizations write to urge your support and swift consideration by the House and Senate Committees on the Judiciary of The Fourth Amendment Is Not For Sale Act (S.1265 / H.R.2738). This bipartisan legislation, recently introduced by privacy champions in both chambers, is urgent given growing revelations that multiple intelligence and law enforcement agencies are exploiting loopholes in outdated privacy laws by purchasing sensitive information that they would otherwise need a court order to obtain. In doing so, they are circumventing the Constitution, the Congress, and the courts, and threatening the privacy of all people in the United States - especially those in our most vulnerable communities.

Congress has long recognized the sensitivity of certain types of business records, such as those held by phone companies and internet service providers. For decades, the law has prohibited such companies from disclosing customer records to government agencies without a court order or other legal process. When it was revealed that the National Security Agency (NSA) had secretly received permission from the Foreign Intelligence Surveillance Court to collect Americans' phone records in bulk, Congress passed legislation to make clear that intelligence agencies must obtain court orders on a case-by-case basis to access such records.[1] In 2018, the Supreme Court added a further layer of protection for one particularly sensitive type of data, holding that the government must obtain a warrant to compel the production of cell phone location information.[2]

[1] USA Freedom Act of 2015, H.R. 2048, 114th Cong. (2015).
[2] *Carpenter v. United States*, 585 U.S. ___ (2018).

Yet starting in early 2020, investigative news outlets revealed that agencies including Customs and Border Protection,[3] the Drug Enforcement Administration,[4] the Federal Bureau of Investigation,[5] Immigrations and Customs Enforcement (ICE),[6] the Internal Revenue Service,[7] the Secret Service,[8] and others have been simply buying sensitive location information for both criminal investigation and intelligence purposes in contravention of the Fourth Amendment and purportedly exploiting a statutory loophole. To accomplish this, the government relies heavily on third parties, often commercial data brokers, who amass information from millions of people's phones through dating apps, gaming apps, prayer apps, and other applications, all without people's affirmative consent.[9] These entities are not covered by existing federal statutes because those statutes were written before the advent of apps and digital data brokers. And several agencies take the position that the constitutional warrant requirement doesn't apply when the government buys data from a willing seller rather than compelling its production.

As always, this invasion of privacy has the greatest impact on vulnerable groups, including racial and religious minorities as well as those engaged in political protest. Data sources included gaming apps and a Muslim prayer app, which means the datasets almost certainly included data from children and targeted particular religious groups.[10] Members of Congress and journalists have uncovered data brokers tracking people to places of worship and protests, meaning this is information also available for government purchase.[11] This presents a serious risk of chilling every person's exercise of their First Amendment rights. Even when specific groups aren't targeted, the practice generally has a disproportionate impact on communities of color: Asian-Americans disproportionately adopt the devices and services targeted by this practice,[12] while Black and Hispanic[13] communities are disproportionately reliant on cell phones as their sole means to access the internet.[14]

---

[3] https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs
[4] https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel
[5] https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/
[6] https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600
[7] https://www.vice.com/en/article/qj479d/irs-investigation-location-data-no-warrant-venntel
[8] https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street
[9] https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x
[10] https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x
[11] https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-wyden-bicameral-coalition-request-ftc-investigate-advertisers-tracking-americans-at-places-of-worship-and-protests; https://www.wsj.com/articles/lawmakers-urge-ftc-probe-of-mobile-ad-industrys-tracking-of-consumers-11596214541.
[12] https://www.nielsen.com/us/en/press-releases/2018/asian-american-consumers-are-predictive-adopters-of-new-media-platforms/
[13] https://www.pewresearch.org/fact-tank/2019/08/20/smartphones-help-blacks-hispanics-bridge-some-but-not-all-digital-gaps-with-whites/
[14] https://www.pewresearch.org/internet/fact-sheet/mobile/?menuItem=d40cde3f-c455-4f0e-9be0-0aefcdaeee00

Disturbing questions remain about the nature and scope of this surveillance, as well as the claimed legal basis for the practice.[15] As we write to you, news is breaking that the Department of Defense and the National Security Agency have wrongfully classified answers to questions from Senator Wyden about whether the government is also exploiting this same loophole or related ones to purchase sensitive location data from cars and internet browsing and search histories of people in the United States.[16] A memo recently obtained from the Defense Intelligence Agency makes the chilling claim that it is lawful to purchase such sensitive data in "bulk."[17]

We urge the House and Senate Committees on the Judiciary to pass legislation ending these alarming practices and to reaffirm the legal restrictions put in place by Congress and the courts. The committees can take a significant step in that direction by advancing the Fourth Amendment Is Not For Sale Act, which would prohibit law enforcement and intelligence agencies from purchasing communications content, geolocation information, and other highly sensitive data. The bill also would limit the government's ability to concoct new and constitutionally unsound workarounds in the future by establishing that the mechanisms provided in statute are the exclusive means by which the government may acquire such information about people in the United States.

In short, the Fourth Amendment Is Not For Sale Act would fill a major gap in statutory law, shoring up Americans' privacy and preventing the use of our tax dollars to fund an industry that spies on innocent people en masse. We support the bill, and we hope we can count on you to lead on this critical issue by advancing the legislation through committee.

Sincerely,

Access Now
American Civil Liberties Union
American Society of Journalists and Authors
Americans for Financial Reform
Americans for Prosperity
Brennan Center for Justice at NYU School of Law
Center for Democracy & Technology
Defending Rights & Dissent

---

[15] https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant
[16] https://www.vice.com/en/article/88ng8x/pentagon-americans-surveillance-without-warrant-internet-browsing
[17] https://int.nyt.com/data/documenttools/dni-to-wyden-on-commercially-available-smartphone-locational-data/5d9f9186c07993b6/full.pdf

Demand Progress
Demos
Due Process Institute
Electronic Frontier Foundation
Fight for the Future
Free Press Action
Free Speech Coalition
FreedomWorks
Government Information Watch
National Coalition Against Censorship
New America's Open Technology Institute
Open The Government
Media Freedom Foundation
MediaJustice
MPower Change
National Association of Criminal Defense Lawyers
PEN America
Project Censored
Project On Government Oversight
Project for Privacy & Surveillance Accountability
Restore The Fourth
RootsAction.org
Surveillance Technology Oversight Project
Woodhull Freedom Foundation
X-Lab

CC: Members of the Senate Committee on the Judiciary
Members of the House Committee on the Judiciary