Free Press Action

Support the Fourth Amendment Is Not For Sale Act (H.R. 4639)

Why We Need H.R. 4639:

- Intelligence and law enforcement agencies are buying our personal information from data brokers, circumventing the Fourth Amendment's warrant requirements. Agencies do this because the relevant federal statutes were written at a time when apps and digital brokers did not exist in anything like the forms they take today, and therefore these laws do not specifically prohibit such actions.

- The bipartisan Fourth Amendment Is Not For Sale Act (H.R. 4639), sponsored by Reps. Nadler, Lofgren, Jayapal, and Jacobs, as well as Reps. Davidson, Biggs, Buck, and Massie, would stop the harmful and unconstitutional sale of personal information to government authorities without a warrant.

- The American public overwhelmingly supports requiring government agencies to get a warrant to access or buy information about people's locations. Per *The Wall Street Journal*, "77% of Americans believe the government should get a warrant to buy the kind of detailed location information that is frequently purchased and sold on the commercial market by data brokers."

- With the rise of the digital age, data collected about us is more meaningfully linked to our basic rights than ever. No matter the efficacy of electronic communications privacy laws that regulate direct disclosure of our data to law enforcement by companies like AT&T, Comcast, Google, or Meta, vast troves of data from these kinds of corporations regularly flow to the government through data brokers and aggregators. That lets government agencies go around Fourth Amendment safeguards by simply asking or paying for the data directly from these brokers.

- The privacy violations that flow from law enforcement entities circumventing the Fourth Amendment have harmful impacts on civil liberties, free expression, and our ability to control what happens to our data. These harms affect all who use digital platforms and give up control of our personal information (often without realizing it) when we open a browser, go to social media and other websites, or even when we go to real-life events like demonstrations and other locations with our phones in tow and revealing our location.

- The Fourth Amendment protects our expression and our rights to association from these kinds of unreasonable invasions of privacy. The plain text of the Fourth Amendment guarantees the security of not just our persons and property, but our "papers" as well, in reaction to the British government entering people's homes to inspect their writings and belongings when people were suspected of being disloyal to the crown.

Implications for Civil Liberties & Free Expression:
Without H.R. 4639, intelligence and law enforcement agencies will continue to exploit this data broker loophole in furtherance of impermissible surveillance. Such government monitoring disproportionately impacts people of color, immigrants, abortion seekers, LGBTQIA+ individuals, political dissidents, and other groups historically and presently targeted by law enforcement and intelligence agencies.

- *Surveillance of demonstrations & activism*: The US government has a long history of abusing surveillance tools to intimidate and undermine activists and social movements. In the 20th century, the FBI's COINTELPRO surveilled and attempted to discredit organizations and activists it considered "subversive," including Martin Luther King Jr. After 9/11, law enforcement surveilled and infiltrated Muslim American organizations, spurring unfounded government investigations and a climate of distrust and fear. Most recently, federal and local law enforcement have engaged in systematic surveillance of Black Lives Matter demonstrators.
    - Phoenix police have used surveillance cameras, license plate readers, and drones to track leaders of a peaceful Black Lives Matter protest for hours, waiting for them to engage in any conduct that could provide a pretext to arrest them, such as stepping off the sidewalk onto a roadway during a demonstration.
    - New York police have used facial recognition software to track a protester to his home, where dozens of officers attempted to forcibly enter without a warrant because he allegedly loudly shouted into a bullhorn at an officer during a demonstration.

- *Surveillance of abortion and healthcare seekers*: In a post-*Roe* United States, we face the reality that location-based online data will become weaponized by those seeking to investigate and charge abortion seekers. Law enforcement and prosecutor access to this data is practically limitless, with examples of local prosecuting offices using location data to bring criminal charges against individuals who have sought abortions in states where abortion has become illegal.

- *Surveillance of religious freedom*: Reporters discovered that the U.S. military was purchasing information from a Muslim prayer app, as well as other apps used by Muslims and by other groups, via the data broker X-Mode, with apparently vast quantities of location data from these innocuous apps fed directly into U.S. military intelligence programs.

Congressional and Agency Efforts on Surveillance & Lax Data Security Practices:

- Congress is currently considering a wide array of comprehensive and more targeted commercial privacy bills. There is a vital need for new comprehensive laws requiring companies to minimize their data collection and prohibiting them from discriminatory data processing. But those bills will not and cannot readily prohibit law enforcement and intelligence agencies from evading the Fourth Amendment the way that the Fourth Amendment Is Not For Sale Act does.

- The FTC is charged with oversight of unfair or deceptive practices related to the harvesting, sharing or sale of personal data, including health-related information, but while that agency is fortunately moving to propose and adopt new rules in this regard it likewise cannot close the data brokers loophole that law enforcement agencies are exploiting.