The Data Broker Loophole is a Threat to Civil Rights

Law enforcement and intelligence agencies have a long record of abusing warrantless surveillance to violate civil rights

Law enforcement and intelligence agencies are now exploiting purchased data to evade privacy protections enacted by Congress and conducting surveillance that the Supreme Court has held violates the Fourth Amendment.

Public reporting shows an increasing number of government agencies warrantlessly buy information about the location and internet activity of people in the U.S, circumventing the privacy protections established in *Carpenter v. United States*. The IRS, Department of Homeland Security, FBI, Department of Defense including Customs and Border Protection and Immigration and Customs Enforcement, and Secret Service have all purchased data using the Data Broker Loophole.

The Data Broker Loophole is a severe threat to civil rights, especially of protestors:
This information, surreptitiously scraped from people's phones and internet activity, reveals incredibly intimate details of a person's life without their consent, including their engagement with protests and social causes, their race and ethnicity, political affiliations and beliefs, familial connections, sexuality and gender identity, financial situation, and even their immigration status and reproductive health care needs.

Government agencies and the U.S. criminal legal system have a long history of discrimination against marginalized communities. Buying access to this sensitive information further endangers already vulnerable people.

Warrantless Surveillance via Data Purchases Sidesteps Fourth Amendment Protections

- The Fourth Amendment protects against general warrants, which gave blanket permission to conduct searches without individualized suspicion of wrongdoing. Buying sensitive information from data brokers, especially in bulk, poses the same threats as, and sometimes is virtually identical to, the issuance of general warrants.
- Buying access to personal information is the digital equivalent of law enforcement paying a company to search a person's personal effects because the police did not have the lawful authority to do so themselves — however, data brokers do this on a massive scale.

Purchased Data Is Weaponized Against Vulnerable Groups and Undermines their Tools of Resistance

- When obtained by law enforcement, purchased data can be used to surveil, arrest, and incarcerate marginalized communities. Privacy is critical for these communities to protect themselves from violence.
- Government purchases of data broker information create massive additional risks for communities that data brokers already harm by supercharging impacts on people disproportionately targeted by our criminal legal system.
- **The Data Broker Loophole is an acute threat to protestors.** Purchased information has been used by police to monitor and track the behavior and location of peaceful protestors. This undermines the First Amendment right to assembly and the democratic values of this country.