Closing the Data Broker Loophole:

GOVERNMENT EVASION OF THE FOURTH AMENDMENT

SUMMARY

Government agencies have evaded the Fourth Amendment using the third-party doctrine as a loophole, enabling an unchecked surveillance state powered by data brokers. Congress must move fast to close the data broker loophole.

WHAT IS THE FOURTH AMENDMENT?

The Fourth Amendment requires the government to get a warrant to access information for which individuals have a "reasonable expectation of privacy." The government exploits the third-party doctrine to bypass Fourth Amendment rights, arguing that individuals lose any expectation of privacy when they voluntarily disclose information to third parties. The third-party doctrine is increasingly incompatible with our digital reality in which devices collect vast amounts of highly sensitive data on Americans.

WHAT ARE DATA BROKERS?

Data brokers collect detailed profiles of personal information, including demographic information, geolocation data, healthcare data, and browsing history. Data brokers profit from selling Americans' private data to government agencies.

EXAMPLES OF GOVERNMENT PARTNERSHIP WITH DATA BROKERS

- Customs and Border Protection previously bought US travelers' domestic flight records from a major airlines-owned data broker, which included passenger names, full flight itineraries, and financial details to track people of interest.
- Law enforcement purchased location data collected from social media platforms to track protesters in Ferguson, Missouri, and Baltimore, Maryland.
- IRS purchased cellphone location data of millions of Americans from data brokers to try to find potential criminal suspects and was unsuccessful.

LACK OF PROTECTIONS

Federal privacy laws generally do not regulate the commercial aggregation of personal data nor the sale of that data to government agencies. Some statutes address parts of the problem, but they only apply to certain sectors or specific types of personal information, tackling only the tip of the iceberg.

CONGRESS MUST REIN IN GOVERNMENT SURVEILLANCE AND DATA BROKERS

Congress should limit data brokers' collection, use, retention, and disclosure of personal data.

Congress should also create guardrails on government agencies' ability to purchase "Fourth Amendment protected information" from any entity. Congress should pass the protections outlined in the **Fourth Amendment Is Not For Sale Act (FAINFSA)**.

FOR MORE INFORMATION

https://epic.org/issues/privacy-laws/fourth-amendment/;
https://epic.org/issues/consumer-privacy/data-brokers/

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

WORKS CITED

1. Bennett Cyphers, “How the Federal Government Buys Our Cell Phone Location Data,” Electronic Frontier Foundation, June 13, 2022, https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data.
2. See Katz v. United States, 389 U.S. 347 (1967).
3. Brennan Center for Justice et al., "Joint Comment Regarding the Office of Management and Budget’s Request for Information on Executive Branch Agency Handling of Commercially Available Information," December 16, 2024, https://epic.org/documents/join-comment-regarding-ombs-request-for-information-on-executive-branch-agency-handling-of-commercially-available-information/.
4. Emile Ayoub and Elizabeth Goitein, “Closing the Data Broker Loophole,” Brennan Center for Justice, February 13, 2024, https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.
5. Joseph Cox, “Airlines Don’t Want You to Know They Sold Your Flight Data to DHS,” Wired, June 10, 2025, https://www.wired.com/story/airlines-dont-want-you-to-know-they-sold-your-flight-data-to-dhs/.
6. Matt Cagle, “Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color,” ACLU Northern California, October 11, 2016, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.
7. Bryon Tau, “IRS Used Cellphone Location Data to Try to Find Suspects,” Wall Street Journal, June 19, 2020, https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815.