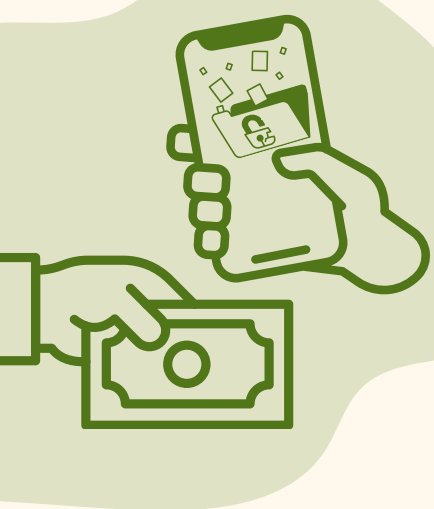

DATA BROKER THREATS: NATIONAL SECURITY

The data broker industry is a threat to national security. The Consumer Financial Protection Bureau has a solution.

SUMMARY

Data brokers build extensive dossiers of information on Americans, including members of the armed forces.

Personal data is collected as we browse the internet and use online services, including location records, biometric data, and health and financial info. Companies sell that info to data brokers, who compile records, draw inferences, and resell datasets and dossiers

The lack of meaningful restrictions on data brokers allows foreign adversaries to purchase detailed records about service members and other government officials, which has revealed sensitive national security information like patrol routes around military bases.

Bad actors use information from data brokers to blackmail or use phishing tactics to obtain state secrets.

EXAMPLES

- Duke University researchers found that data brokers sell sensitive data about active-duty military members, veterans, and their families for as little as $.12 per record.
- The Irish Council for Civil Liberties found that foreign adversaries can obtain sensitive data about U.S. service members, politicians, and other high-profile figures through the real-time bidding system used by data brokers to target online advertisements.
- In 2018, researchers and activists found that Strava's global heat map showing user activity records could be used to identify the locations of military bases and patrol routes, as well as identifying information for the service members who used Strava in those locations.

FOR MORE INFORMATION

https://epic.org/cfpb-fair-credit-reporting-act-rulemaking/

NEW DATA BROKER RULES WILL REDUCE THREATS TO NATIONAL SECURITY

New rules being considered by the Consumer Financial Protection Bureau would clarify that data brokers are covered by the Fair Credit Reporting Act, meaning that data brokers can only collect consumer information for a limited number of permissible purposes. The rules would also clarify that data brokers can only share data they collect with third parties for permissible purposes.

Minimizing the data that brokers amass and sell in the first place is a powerful national security safeguard: you don't have to protect what you don't collect.

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

WORKS CITED

1. Exec. Order No. 14117, 28 C.F.R. 202 (Mar. 1, 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.
2. Prepared Remarks of CFPB Director Rohit Chopra at the White House on Data Protection and National Security, CFPB (Apr. 2, 2024), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-at-the-white-house-on-data-protection-and-national-security/.
3. Justin Sherman, Hayley Barton, Aden Klein, Brady Kruse, & Anushka Srinivasan, Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security, (Duke Univ. Sanford School of Public Policy eds. Nov. 2023), https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.
4. Johnny Ryan & Wolfie Christl, America's Hidden Security Crisis: How Data About United States Defence Personnel and Political Leaders Flows to Foreign States and Non-State Actors (Irish Council for Civil Liberties eds. Nov. 2023), https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-security-crisis.pdf.
5. Jeremy Hsu, The Strava Heat Map and the End of Secrets, Wired (Jan. 29, 2018), https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.
6. Small Business Advisory Review Panel for Consumer Reporting Rulemaking: Outline of Proposals and Alternatives Under Consideration, CFPB (Sept. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf.