

July 13, 2023

Senator Maria Cantwell
Chair
Senate Committee on Commerce, Science,
and Transportation

Representative Cathy McMorris Rodgers
Chair
House Committee on Energy and Commerce

Senator Ted Cruz
Ranking Member
Senate Committee on Commerce, Science,
and Transportation

Representative Frank Pallone
Ranking Member
House Committee on Energy and Commerce

Dear Sen. Maria Cantwell, Rep. Cathy McMorris Rodgers, Sen. Ted Cruz, and Rep. Frank Pallone:

Recent reports suggest that lawmakers are considering changes to the proposed American Data Privacy and Protection Act (ADPPA) that would exempt data brokers who provide services to law enforcement agencies.¹ These proposed changes would dramatically infringe upon the civil liberties of Americans, providing law enforcement with tools for surveillance and prosecution without the need for a warrant or due process. We urge you to reject any amendment to the ADPPA that would permit law enforcement to sidestep constitutional protections by purchasing Americans' private data.

Over the past several years, journalistic reporting,² congressional inquiries,³ and federal agencies themselves⁴ have shed light on the extent to which U.S. law enforcement and intelligence agencies rely on data obtained from the private sector. Through data brokers, law enforcement may purchase geolocation information and online browsing histories, all with enough precision to attribute personal identities to the data.⁵ While close surveillance by government entities routinely requires a warrant with "probable cause," the purchase of commercially-available data has no such safeguards.

The government's acquisition of private data flies in the face of Americans' constitutional rights. As lawmakers from both parties noted at a House Judiciary hearing last year, the warrantless purchase of private data represents a break with due process, an infringement on Fourth Amendment liberties, and an abuse of government power.⁶

¹<https://subscriber.politicopro.com/article/2023/06/lawmakers-are-debating-a-law-enforcement-exemption-for-data-brokers-in-privacy-bill-00102016>

²<https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>

³<https://www.congress.gov/event/117th-congress/house-event/115009>

⁴<https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf>

⁵<https://www.wsj.com/articles/u-s-spy-agencies-buy-vast-quantities-of-americans-personal-data-report-says-f47ec3ad>

⁶<https://judiciary.house.gov/committee-activity/hearings/full-committee-hearing-on-privacy-and-government-surveillance>

While all Americans are impacted by the exposure of their private data to law enforcement and intelligence agencies, marginalized communities are often the hardest hit. For example, the military has purchased sensitive geolocation data gathered from Muslim prayer and dating apps in order to track users.⁷ The broker that sold the user geolocation data, Locate X, boasts of being “widely used” by the military, intelligence agencies, and law enforcement. Immigration and Customs Enforcement (ICE) also has a history of purchasing user data in order to track migrants and skirt sanctuary laws.⁸

Following the Supreme Court’s decision in *Dobbs v. Jackson*, law enforcement agencies in states with an abortion ban are also using private data to track and prosecute women seeking reproductive care.⁹ As a recent report by the Congressional Research Service notes, “federal data privacy law provides relatively limited constraints upon law enforcement’s ability to acquire privacy data relating to criminal activity, potentially including abortion activity.”¹⁰ While President Biden has taken executive action to protect HIPAA data from being sold by data brokers, non-HIPAA health data, geolocation data, and other commercial data is still available for purchase by law enforcement for use in prosecuting abortion cases.

Lobbyists for the data broker industry have stressed national security concerns regarding the ADPPA’s restrictions preventing law enforcement from buying private data, saying that such a prohibition would put the U.S. at a disadvantage against its adversaries. But the maintenance of Americans’ civil liberties should never be considered a disadvantage. While China and Russia may employ vast surveillance states, the United States’ safeguards against surveillance, while incomplete, enable a healthy and robust democracy which is in fact our nation’s strongest asset.

As you continue to negotiate national legislation protecting Americans’ digital privacy, we urge you to avoid creating loopholes for law enforcement and intelligence agencies that would enable the invasion of privacy, the abridgement of due process, and the miscarriage of justice. Enacting national privacy safeguards should be a top legislative priority for both parties, but there is no reason that such legislation should come at the cost of Americans’ civil liberties.

Sincerely,

Chamber for Progress
Asian Americans Advancing Justice - AAJC
LGBT Tech
UnidosUS

⁷<https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>

⁸<https://www.washingtonpost.com/politics/2022/07/27/ices-use-data-brokers-go-around-sanctuary-laws-under-fire/>

⁹<https://www.businessinsider.com/police-getting-help-social-media-to-prosecute-people-seeking-abortions-2023-2>

¹⁰<https://crsreports.congress.gov/product/pdf/LSB/LSB10786>