July 19, 2022

Representative Jerrold Nadler, Chairman
Representative Jim Jordan, Ranking Member
U.S. House Committee on the Judiciary

Re: Hearing on "Digital Dragnets: Examining the Government's Access to Your Personal Data"

Dear Chairman Nadler, Ranking Member Jordan and Esteemed Committee Members:

We the undersigned members of the Disinfo Defense League respectfully request that you accept this letter for the record of your July 19, 2022, hearing on "Digital Dragnets: Examining the Government's Access to Your Personal Data."

The Disinfo Defense League, or DDL, is a distributed national network of over 230 grassroots, community-based organizations that are building a collective defense against disinformation campaigns that deliberately target Black, Latinx, Asian American, and other communities of color.

We are deeply concerned by systemic problems posed by the complex set of digital tactics, extractive data practices, and manipulative tech platform and app designs that undermine confidence in our democracy, sow distrust among Americans in our public health institutions, disenfranchise voters, and chill engagement for our communities. All of these practices contribute to the weaponization of online narratives that target our communities.

The impact on real people is not abstract. Data brokers gather incredibly private details like individuals' sex, age, gender, geolocation, and health information; they can also collect internet-search histories that reveal even more sensitive information about people. This data is accessible to any intelligence community entities with the dollars to spend for it. And when private data brokers collect information about us, that information is available for the government to purchase – a loophole which circumvents any court oversight.

That loophole should be closed. Earlier this Congress, Chairman Nadler introduced the Fourth Amendment Is Not for Sale Act, H.R. 2738, co-sponsored by Rep. Zoe Lofgren. Passing this bill and making it law would be an excellent start to preventing platforms and data brokers from selling people's personal information to law enforcement and intelligence agencies without a warrant or any other court oversight.

To build criminal cases against individuals, law enforcement purchases from data brokers a wide range of sensitive data points. That can be our location history showing a visit to a mental-health facility, house of worship, public protest and beyond. It can also include our search engine histories, our health information, app usage, and phone calls.[1]

For government officials to do this without a warrant violates the spirit of this country's commitment to privacy and to freedom of thought and expression. As far back as this country's founding, the Fourth Amendment was conceived as a protection against what people had experienced during early British rule, during which crown officials entered people's homes, and inspected their writing and belongings whenever they were suspected of being disloyal to the king.

In this digital age, the unfettered access law enforcement has to almost all of our digital footprints is of deep concern. And, as is always the case sadly, it's fair to conclude that the people who are going to be the most criminalized by this evidence are going to be people of color. Stanford Open Policing Project has found that Black drivers across the United States are 20 percent more likely to be stopped than white drivers. In addition, the Armed Conflict Location & Event Data Project (ACLED) found that although over 94 percent of racial justice protests have been peaceful since 2020, authorities are three times more likely to intervene in pro-Black Lives Matter demonstrations than they are in other demonstrations. And, when intervening, police used force against pro-BLM demonstrators 52 percent of the time, compared to 26 percent of the time against all other demonstrators. These studies point to the harsher treatment law enforcement gives to people of color, a symptom of how our intelligence and law enforcement officials treat communities of color both with and without the aid of technology or purchased access to our data.

We are encouraged by this Committee's efforts to provide guardrails around the use and sale of people's personal data and to mitigate the rise of "digital dragnets." We need interventions from Congress to protect Americans against violative invasions of privacy such as those you are called to discuss today.

[1] One example of data purchases surfaced in 2020, when it was discovered that the U.S. military was purchasing information from a Muslim prayer app. *See* Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *Motherboard*, Nov. 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

Companies need to disclose not just what information they collect, but where they get the information; who shares data with them, and with whom they share data; how they analyze data to profile us; how else they use our information; how they make decisions about what content, goods or services to offer us; and how they secure our data. Then we need to make sure that government is not on the list of entities they share with, at least in the absence of a warrant.

While there's more work to be done to holistically safeguard privacy and civil rights online, we write today to urge the Committee to pass the Fourth Amendment Is Not For Sale Act. The Disinfo Defense League has long championed this legislation in our Policy Platform,[2] sounding the alarm about nefarious data practices which violate our fundamental privacy rights. The DDL platform codifies policy principles designed to rein in technology companies' extractive data practices and to safeguard privacy and civil rights on social media platforms with comprehensive digital-privacy measures.

Now is the moment for Congress to enact robust protections against digital dragnets and to advance a civil rights agenda for all online users. We look forward to further discussion about these issues and hope to see the Fourth Amendment Is Not For Sale become law.

Respectfully submitted,

Access Humboldt
Access Now
Asian Americans Advancing Justice – AAJC
Center for Countering Digital Hate
Common Cause
Fight for the Future
Filipino Young Leaders Program (FYLPRO)
Free Press Action
Indivisible Bainbridge Island
Indivisible Plus Washington
Lower Columbia Indivisible
MediaJustice
Muslim Advocates
New Georgia Project Action Fund
NYU Cybersecurity for Democracy

[2] Disinfo Defense League, Policy Platform (Dec. 7, 2021), https://www.disinfodefenseleague.org/policy-platform.

Snohomish County Indivisible
UCLA Center for Critical Internet Inquiry
Voto Latino
WA People's Privacy Network