Congress of the United States
House of Representatives
Washington, DC 20515

December 9, 2021

Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20554

Jessica Rosenworcel
Chair
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Dear Chair Khan and Chair Rosenworcel:

We write to urge the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) to develop new rules against the collection and sale of consumers' location data. Currently, app developers are able to collect sensitive user information and sell it to interested parties for a substantial profit. Apps can harvest personal information, such as geolocation and phone identifiers, even after users denied permission for such sharing, according to one study published on the FTC's website.[1] We are concerned that the continued, unregulated commercialization of private geolocation data compromises the safety and privacy of consumers.

The vast majority of American consumers are concerned about how companies use the data they collect from them.[2] Users who belong to historically marginalized groups may face higher stakes when their data privacy is violated. Women, especially survivors of domestic violence, face a heightened risk of being cyberstalked. About 75 percent of the victims of stalking and cyberstalking are women.[3] Stalkers can readily purchase their victims' GPS information from data brokers, and a growing number of apps offer location tracking and other stalking functionalities.[4] As former FTC chief technologist Ashkan Soltani said, data brokerage is "a multibillion-dollar industry that feeds off [user] data and profits from the sale of it." These incidents point to gaps in our current regulatory framework, which is failing to adequately protect consumers from discrimination and abuse.

In a high-profile privacy incident from earlier this year, a Catholic media site used commercially available app data to out a Catholic Church official, resulting in his resignation. The site's investigation correlated app data signals from the dating app Grindr to the official's mobile

[1] "50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System," Federal Trade Commission at: https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf (2019)
[2] "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center at: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (November 2019)
[3] "What Women Know About the Internet," New York Times at: https://www.nytimes.com/2019/04/10/opinion/privacy-feminism.html (April 2019)
[4] "Hundreds of Apps Can Empower Stalkers to Track Their Victims," New York Times at: https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html (May 2018)

device at multiple locations including his home, place of work, and gay bars.[5] While commercially sold app signal data does not typically identify users by name, it contains numerical identifiers of mobile devices and can be readily de-anonymized. Mobility data, as well as information like an individual's home and work addresses, can also be used to deconstruct anonymized data.[6]

In the past, both FTC and FCC punished bad actors for failing to safeguard location data, but the agencies fell short of establishing prophylactic rules that will better protect consumers. Last year, the FCC proposed more than $200 million in fines against the four largest wireless carriers in the country for selling their customers' location information to data brokers.[7] At the time, then Commissioner, now Chairwoman Rosenworcel observed that "[o]ur real-time location information is some of the most sensitive data there is about us, and it deserves the highest level of privacy protection."[8] More recently, the FTC banned the stalkerware app SpyFone, in part because the app "illegally harvested and shared people's private information without consent" for its subscribers.[9]

While we applaud the agencies' commitments to consumer privacy and safety, it is clear that more needs to be done. To that end, we ask that your agencies take the following steps to better protect the safety and privacy of consumers:

1. The FTC should define the sale, transfer, use, or purchase of precise location data collected by an app for purposes other than the essential function of the app as an "unfair act or practice" through its Section 18 rulemaking authority.

This would severely constrain the use of software development kits that trade their functionality in exchange for commercially valuable location data. At a minimum, app developers should be required to obtain express, informed user consent for separate data usage, and any such use should be opt-in only.

2. The FTC should define app developers' mislabeling of users' location data as "anonymous" as a "deceptive practice" through its Section 18 rulemaking authority.

By claiming users' location data will be anonymous, app developers are failing to convey how collected data can be traced back to the user with de-anonymization tactics, instilling a false

[5] "Top U.S. Catholic Church official resigns after cellphone data used to track him on Grindr and to gay bars," The Washington Post at: https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/ (July 2021)
[6] "Unique in the Crowd: The privacy bounds of human mobility," Nature at: https://www.nature.com/articles/srep01376 (March 2013)
[7] "FCC proposes roughly $200 million in fines against wireless carriers for mishandling customers' location data," The Washington Post at: https://www.washingtonpost.com/technology/2020/02/28/fcc-proposes-roughly-200-million-fines-against-wireless-c arriers-mishandling-customers-location-data/ (February 2020)
[8] https://docs.fcc.gov/public/attachments/FCC-20-25A4.pdf (February 2020)
[9] "FTC action against stalkerware app SpyFone and CEO Scott Zuckerman underscores threats of surveillance businesses," Federal Trade Commission at: https://www.ftc.gov/news-events/blogs/business-blog/2021/09/ftc-action-against-stalkerware-app-spyfone-ceo-scott (September 2021)

sense of security. Without this understanding, users are being misled into believing their data cannot be traced back to them.

3. The FTC should enforce the above regulations against companies abusing consumers' location data through its Section 5(m) authority.

Penalties punish bad actors, reinforce the FTC's authority, and deter companies from exploiting consumers. Assigning penalties is one of the most effective and efficient ways for the FTC to enforce the law, yet the FTC has rarely used this penalty authority over the last four decades.[10] The FTC needs to substantially step up its protection of consumer privacy.

4. The FCC should protect consumers' geolocation information by reaffirming its prohibitions on the surveillance of location data through rulemaking.

In 2013, the FCC issued a declaratory ruling clarifying that the customer proprietary network information (CPNI) protections apply to information collected from a mobile device, including "the location of a customer's use of a telecommunications service." In recent enforcement decisions the FCC also found that the customer location information at issue fell squarely within Section 222 of the Communications Act's definition of CPNI. We urge the FCC to reaffirm these findings as it pursues its enforcement and policy agenda, including through future rulemaking.

We recognize that any rulemaking on privacy protections for consumers' location data will be most effective when the FTC and FCC work together to combine their adjacent authorities. We look forward to your response.

Sincerely,

Katie Porter
Member of Congress

Jamie Raskin
Member of Congress

Ayanna Pressley
Member of Congress

Raul Grijalva
Member of Congress

Adam Schiff
Member of Congress

Ed Case
Member of Congress

Pramila Jayapal
Member of Congress

Jackie Speier
Member of Congress

Ted Lieu
Member of Congress

Mondaire Jones
Member of Congress

Alexandria Ocasio-Cortez
Member of Congress

[10] "What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities," Electronic Privacy Information Center at: https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf (June 2021)

Grace Meng
Member of Congress

Robin Kelly
Member of Congress

Eleanor Holmes Norton
Member of Congress

Gwen Moore
Member of Congress

Marc Veasey
Member of Congress

Jesús G. "Chuy" García
Member of Congress

Alan Lowenthal
Member of Congress

Gregory W. Meeks
Member of Congress

Norma Torres
Member of Congress

Mark Takano
Member of Congress

Dina Titus
Member of Congress

Albio Sires
Member of Congress

Suzanne Bonamici
Member of Congress

Mark Pocan
Member of Congress

Sanford D. Bishop, Jr.
Member of Congress

Andy Levin
Member of Congress

Rashida Tlaib
Member of Congress

Mary Gay Scanlon
Member of Congress

Donald Payne, Jr.
Member of Congress

Jim Cooper
Member of Congress

Stephen F. Lynch
Member of Congress

Danny K. Davis
Member of Congress

Henry C. "Hank" Johnson, Jr.
Member of Congress

Earl Blumenauer
Member of Congress

Yvette D. Clarke
Member of Congress

Mark DeSaulnier
Member of Congress

Pete Aguilar
Member of Congress

Carolyn Maloney
Member of Congress

Al Green
Member of Congress

David Trone
Member of Congress

Sheila Jackson Lee
Member of Congress

Shontel Brown
Member of Congress

Rick Larsen
Member of Congress