815 Eddy Street
San Francisco, CA 94109
www.eff.org | (415) 436-9333

**MEMORANDUM**

**Date:** Friday, May 26, 2023
**To:** All Asssembly Members, New York State Assembly; All Senators, New York State Senate
**From:** Chao Jun Liu, Legislative Associate, Electronic Frontier Foundation

**Re: Electronic Frontier Foundation Memorandum in Support of A3306/S217**

I write today on behalf of the Electronic Frontier Foundation (EFF), a San Francisco-based, non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 35,000 active donors and members, including thousands of supporters in New York. We write in support of Assembly Bill 3306 and Senate Bill 217, which would put a stop to unconstitutional "reverse demands," protecting New Yorkers from overbroad law enforcement surveillance.

**"Geofence Demands" Trample the Rights of Innocent People**

Location surveillance comes with a host of risks to citizens' privacy, freedom of expression and data protection rights. EFF has long fought against granting law enforcement agencies access to location data or blanket data retention mandates, and has called on governments to be more transparent on their surveillance programs.

Geofence warrants, which have already been used against protestors, allow law enforcement to gather data about any number of devices in a given area.[1] The area covered can range from a single building to the equivalent of 24 football fields, with a time period ranging from a few hours to a week.[2] These devices are then linked to real people, many of whom have no ties to criminal activity, and for whom the government has demonstrated no probable cause to search.

EFF believes these kinds of searches clearly violate the Fourth Amendment, even when they are conducted with a warrant. Such warrants allow broad fishing expeditions, the very type of searches that the Fourth Amendment – which states warrants must "particularly describe[e] the place to be searched, and the persons or things to be seized" – is designed to prevent. From a single warrant, police access exponentially more detailed

[1] Russell Brandom, "How Police Laid Down a Geofence Dragnet for Kenosha Protestors." The Verge (August 30, 2021), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake
[2] Jennifer Lynch and Andrew Crocker, "People v. Meza – Geofence Warrant – EFF Amicus Brief in Support of Appellant at California Court of Appeal," Electronic Frontier Foundation (Jan 24, 2023): pp27-31 https://www.eff.org/document/people-v-meza-geofence-warrant-eff-amicus-brief-support-appellant-california-court-appeal

information than they ever could in the past from more devices than ever before. More often than not, this all happens without the knowledge of the people whose lives have been placed under extreme scrutiny.

**"Keyword Demands" Are Similarly Unconstitutional**

With a "keyword" warrant, police compel companies like Google to hand over the identities of anyone who may have searched for a specific term, such as a victim's name or a particular address where a crime has occurred. Like geofence warrants, these are fishing expeditions without particularized suspicion.

Today many people routinely rely on search engines to search for answers to their most mundane and most intimate questions.[3] Just as where we go can reveal who we associate with, how we worship, and even the state of our health, what we search for can and does reveal similarly sensitive information. Or an idle Google search for an address that corresponds to the scene of a robbery could make you a suspect. Keyword searches potentially implicate all the innocent people who just happened to have searched for something now of interest to the police.

**Warrants Do Not Stop These Privacy Harms**

Reverse searches implicate innocent people and have a real impact on people's lives. Even if you can later clear your name, if you spend any time at all in police custody, this could cost you your job, your car, and your ability to get back on your feet after the arrest.

Warrants alone are not enough to protect our privacy, especially when many courts simply rubber stamp warrant request without questioning their scope.[4] Thus, it is the role of the legislature to end these practices. That is why EFF supports A.3306 and S.217.

We thank you for addressing this important issue with strong legislation that New Yorkers need. We respectfully urge the legislature to pass these bills. If you have any questions or would like to discuss anything I have said in more detail, please contact me at chao@eff.org or 415-436-9333 x171

Sincerely,

[3] Jennifer Lynch and Andrew Crocker, "*UPDATE: Colorado Supreme Court Grants Review in First U.S Case Challenging Dragnet Keyword Warrant*" Electronic Frontier Foundation (June 30, 2022), https://www.eff.org/deeplinks/2022/06/eff-file-amicus-brief-first-us-case-challenging-dragnet-keyword-warrant

[4] Jennifer Valentino-DeVries, "Tracking Phones, Google is a Dragnet for the Police," New York Times (April 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

Chao Jun Liu
Legislative Associate
Electronic Frontier Foundation