MEMORANDUM

Date: Wednesday, January 5, 2022
To: All Assembly Members, New York State Assembly; All Senators, New York State Senate
From: Hayley Tsukayama, Legislative Activist, Electronic Frontier Foundation

Re: Electronic Frontier Foundation Memorandum in Support of A84/S296

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 30,000 active donors and members, including thousands of supporters in New York. We write in support of Assembly Bill 84 and Senate Bill 296, which would place important protections against law enforcement surveillance. These bills will protect New Yorkers from overbroad surveillance.

"Reverse location warrants" 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.

This bill would stop law enforcement from conducting a particularly troubling type of dragnet surveillance on New Yorkers by stopping "reverse location" warrants. Such warrants—sometimes also called a "geo-fence" warrant—allow law enforcement agencies to access data about dozens to hundreds of devices. These devices are linked to real people, many of whom (and perhaps in some cases, all of whom) have no tie 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 cover geographic areas ranging from single buildings to multiple blocks, and time periods ranging from a few hours to a week. Such warrants allow for fishing expeditions, the very type of searches that the Fourth Amendment—which states warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized"—is designed to prevent.

This means that, through a single warrant, the police can access exponentially more and more detailed information about us than they ever could in the past, This means that, through a single warrant, the police can access exponentially more and more detailed information about us than they ever could in the past, and from many more devices. All of this happens, in many cases, without the knowledge of the people whose lives are placed under extreme scrutiny.

Warrants do not stop these privacy harms

Location data is highly sensitive, and can reveal information not only about where we go, but with whom we associate, the state of our health, or how we worship. Reverse location warrant searches implicate innocent people and have a real impact on people's lives. Even if you are later able to 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.

Many courts rubber stamp warrant requests without questioning their broad scope. [1] The use of such broad warrants demonstrate that the warrants alone are not enough to protect our privacy; legislatures must act to stop these practices. That is why we support A84/S296.

We thank you for addressing this important issue with the strong legislation that New Yorkers need. We urge the legislature to pass it. If you have further questions or would like to discuss anything I have said in more detail, please contact me at hayleyt@eff.org or 415-436-9333 x161.

Respectfully submitted,

/s_____
Hayley Tsukayama
Legislative Activist
Electronic Frontier Foundation

---

[1] Valentino-Devries, J. (2019, April 13). Tracking Phones, Google Is a Dragnet for the Police. Retrieved June 16, 2020, from https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html