Legislative Affairs
One Whitehall Street
New York, NY 10004
212-607-3300
www.nyclu.org

2021-2022 Legislative Memorandum

Subject: Prohibits the use of reverse location and reverse keyword searches - A.84 (Quart) / S.296 (Myrie)

Position: SUPPORT

Warrants are a central tool for law enforcement investigations, and they are powerful: they permit the government to obtain private property and communications. In order to prevent warrants from authorizing fishing expeditions that invade our privacy, they must be narrowly targeted, specific, and based on probable cause.

Reverse location and keyword warrants request the disclosure of *multiple* people's private information simply because they were at a particular location during a specific time frame, or entered certain keywords into a search engine. Because they seek to grant the state power to obtain private records that contain information about numerous people, reverse warrants by definition are neither targeted nor specific. Reverse warrants erode the privacy and safety of countless people who just happen to meet the stated criteria – which may be as simple and mundane as using Google or commuting by bike through the virtual perimeter around a location of interest (also known as a "geofence").

Such dragnet warrant requests can place hundreds or thousands of unsuspecting and innocent people in the crosshairs of law enforcement, threatening their Fourth Amendment rights to be free from unreasonable government searches. As technology platforms and data brokers capture ever-more detailed data trails, lawmakers need to ensure these are not exploited by law enforcement to circumvent constitutional checks on police surveillance.

New York has the opportunity to put a stop to this kind of indiscriminate government surveillance. **A.84 (Quart) / S.296 (Myrie)** would prohibit both reverse location and reverse keyword searches and warrants. **The NYCLU strongly supports this legislation and calls for its immediate passage.**

The rapidly increasing threat of reverse warrants.

Computers are everywhere. Whether through phones or other smart devices, such as watches and speakers, vast amounts of data are collected, analyzed, correlated, and shared, capturing intricate details of our lives. But our participation in digital life should not automatically result in the dystopian threat of pervasive police spying.

Shrouded in secrecy, reverse warrant requests have already led to false arrests, highlighting the immense risks of implicit bias and confirmation bias when police utilize these tools.[1] "Geofence" warrants were even used at First Amendment-protected protests against police brutality, throwing digital dragnets over protesters in Minneapolis, Minnesota and Kenosha, Wisconsin.[2]

In response to advocacy by a nationwide coalition of privacy and civil liberties groups,[3] Google released aggregate data about geofence warrant requests from law enforcement across the country from 2018-2020.[4] The report shows a staggering **twelvefold increase** over those three years (*see figure 1*), totaling 20,932 requests. The number of accounts implicated in each of these requests was not disclosed and the requests could easily implicate hundreds of thousands, if not millions, of user accounts and devices.

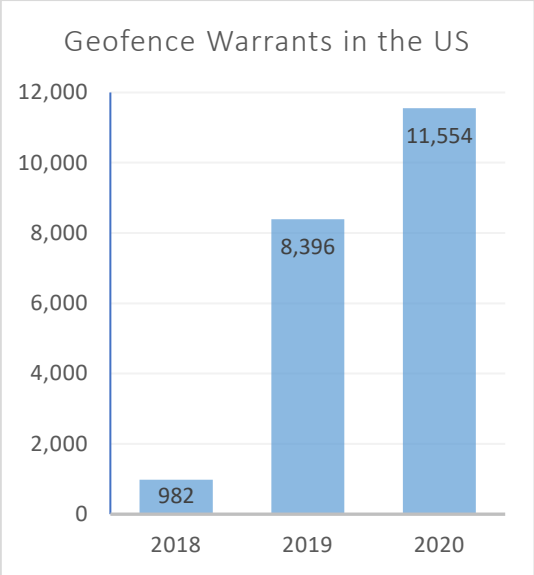

Figure 1: Geofence warrant requests submitted to Google, 2018-2020.

Given the ubiquitous and ever-expanding role that digital technologies play in all our lives, passing A.84/S.296 is urgent. Reverse location and reverse keyword searches are undirected fishing expeditions by law enforcement – made possible by technology that was recently enough inconceivable to policy-makers and impossible to regulate pre-emptively. Where the law lags behind rapid advancements in surveillance technology, our privacy and civil liberties remain at risk unless and until the New York legislature passes legislation to catch up.

The New York Civil Liberties Union strongly supports A.84/S.296 and urges lawmakers to pass it promptly.

---

[1] *See* e.g., Jon Schuppe, *Google tracked his bike ride past a burglarized home. That made him a suspect.*, NBC NEWS (2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761, Meg O'Connor, *Avondale Man Sues After Google* Data Leads to Wrongful Arrest for Murder, Phoenix New Times (2020), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374.

[2] *See* e.g., Zack Whittaker, *Minneapolis police tapped Google to identify George Floyd protesters*, TECHCRUNCH, https://social.techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/, Russell Brandom, *How police laid down a geofence dragnet for Kenosha protestors*, THE VERGE (2021), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake.

[3] Letter to Google on "Geofence" and "Keyword Warrants", NEW YORK CIVIL LIBERTIES UNION (2020), https://www.nyclu.org/en/publications/letter-google-geofence-and-keyword-warrants.

[4] Supplemental Information on Geofence Warrants in the United States, GOOGLE (2021), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf.