

The Legal Aid Society Memorandum in Support of A84-A/S296-A

To: New York State Legislature

From: Diane Akerman, Staff Attorney, Digital Forensics Unit

January 3, 2022

Diane Akerman
Staff Attorney, Digital Forensics Unit
Cell: (646) 634-3094
DAkerman@legal-aid.org

Jerome D. Greco
Supervising Attorney, Digital Forensics Unit
Cell: (646) 946-1648
JGreco@legal-aid.org

Introduction

Since 1876, The Legal Aid Society has provided free legal services to New York City residents who are unable to afford private counsel. Annually, through our criminal, civil and juvenile offices, our staff handles approximately 300,000 cases for low-income families and individuals. The Society serves as the primary defender of indigent people prosecuted in the State court system in New York City.

This memorandum is written in support of A84-A and S296-A, bills sponsored by Assemblymember Dan Quart and Senator Zelnor Myrie to prohibit the search of geolocation data and reverse keyword searches of individuals who are under no particularized suspicion of having committed a crime, and defined only by their mere presence near a location, or their use of certain search terms.

The Use of Reverse Location and Keyword Searches Violates New Yorkers' Right to Privacy and Sweeps Innocent Civilians into Law Enforcement Dragnets

Reverse location searches allow the search of a database to identify mobile devices within a specified geographical limit, known as a geofence.¹ Rather than targeting a specific individual, these searches potentially capture *every device* in a geographic area during a specific period.² Notably, and most commonly, this information is supplied to law enforcement from Google, whose location apps are among the most frequently used by consumers, regardless of the type of device used.³ Reverse keyword searches force a web service, typically an internet search engine, to identify and provide information to law enforcement on anyone who searched a term or set of terms using their service. This amounts to a nationwide violation of people's rights, solely based off the fact that these individuals may have searched a term that law enforcement has deemed relevant to their investigation, regardless of how broad or common the term may be.⁴

¹ Cheryl Meyers Buth & Joel L. Daniels, *Don't Fence Me In-Location Tracking Technologies and the Future of Privacy*, NEW YORK STATE ACADEMY OF CRIMINAL DEFENSE LAWYERS, ATTICUS, VOL. 32, NO. 2, SPRING 2020 at 25.

² Jennifer Lynch & Nathaniel Sobel, *New Federal Court Rulings Find Geofence Warrants Unconstitutional*, ELECTRONIC FRONTIER FOUNDATION (August 31, 2020) (<https://www EFF.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0>) (last accessed December 27, 2021).

³ Buth, *supra* at 26.

⁴ "For keyword search warrants... anyone who searched for a certain phrase or address becomes a suspect. The latter is potentially more far-reaching than geofence warrants... because keyword search warrants are not necessarily geographically or tangibly tied to a specific crime and could make suspects out of people around the world who happened to search for specific terms." Johana Bhuiyan, *The new warrant: how US police mine Google for your location and search history*, THE GUARDIAN (September 16, 2021) (<https://www.theguardian.com/us-news/2021/sep/16/geofence-warrants-reverse-search-warrants-police-google>) (last accessed December 27, 2021).

Individuals have a right to privacy in their physical movements, and recent U.S. Supreme Court cases have continued to uphold this right in the digital context.⁵ Unlike traditional, constitutionally permissible searches, which are limited to specific people, reasonably suspected of criminal activity, geofence searches impose no limit whatsoever on the number of people that may be subject to an invasion of privacy. A single geofence, especially in a place as densely packed as New York, can affect thousands of people, easily tracing their location and identity, even when they are not suspected of any crime. This kind of search is unprecedented in Fourth Amendment history, and is precisely the type of unreasonable search that the Fourth Amendment seeks to prohibit.

The use and misuse of reverse location warrants is far from theoretical - it poses an immediate risk to the personal privacy of millions of New Yorkers. Though its use by law enforcement is relatively new,⁶ Google has observed a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and the rate increased over 500% from 2018 to 2019.⁷ As of 2020, Google reports that geofence warrants requests were up by 50% overall, and in New York State alone were five times higher than in 2018.⁸ Last year, a federal magistrate judge noted that, “[t]he government's undisciplined and overuse of this investigative technique in run-of-the-mill cases that present no urgency or imminent danger poses concerns to our collective sense of privacy and trust in law enforcement officials.”⁹ There has been no public disclosure from Google, Yahoo, or Bing as to the number of reverse keyword search warrants requests received. Public court filings indicate that the practice has been utilized by law enforcement in at least six high profile cases.¹⁰

Courts have failed to prevent the use of reverse warrants, allowing law enforcement to easily amass vast troves of personal privacy data. One court in Virginia approved a warrant application that simply stated that the suspect had a phone in his

⁵ See e.g. *United States v. Jones*, 565 U.S. 400 (2012); *Carpenter v. United States*, 585 U.S. ___, 138 S.Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2017) (requiring warrants for GPS trackers, historical cell site location information, and physical searches of cell phones, respectively); See also *People v. Weaver*, 12 N.Y.3d 433 (2009) (Court of Appeals relies on New York Constitution to suppress warrantless use of a GPS tracker on a vehicle because the defendant had a reasonable expectation of privacy in his locations).

⁶ “The practice was first used by federal agents in 2016, according to Google employees, and first publicly reported last year in North Carolina. It has since spread to local departments across the country, including in California, Florida, Minnesota, and Washington.” Jennifer Valentino-DeVries, *Tracking Phones, Google is a Dragnet for the Police*, NY TIMES (April 13, 2019) (<https://nyti.ms/38XclgU>) (last accessed December 27, 2021).

⁷ *Brief of Amicus Curiae Google LLC in United States v. Chatrie*, 19-cr-00130-MHL (E.D. Va.) (December 23, 2019) (<https://s3.documentcloud.org/documents/6747427/2.pdf>) (last accessed December 27, 2021).

⁸ Google, *Supplemental Information on Geofence Warrants in the United States*, (https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf) (last accessed December 27, 2021).

⁹ *In re Search of Info. Stored At Premises Controlled By Google*, No. 20 M 392 (N.D. Ill. Aug. 24, 2020).

hand during the robbery. That terse recitation led to obtaining private cellphone data for nineteen individuals, at least eighteen of which were not suspected of any wrongdoing.¹¹ In Wisconsin, federal officials successfully sought device information for every person within a 29,387 square meter area over a nine-hour period of time. In response, Google provided 1,494 device identifiers.¹² The few known reverse keyword warrants have used broad search terms, including information previously publicly revealed by law enforcement, that could trap anyone simply curious about the details of a high-profile investigation.¹³

Another troubling report found that judges issued geofence warrants after only four minutes of consideration and were deprived of information that would truly demonstrate the scope and breadth of the proposed search.¹⁴ In a few cases where Google deemed the request inappropriate, law enforcement simply turned to other search engines to obtain the same data – leaving people’s privacy rights to the whims of individual corporate interests.¹⁵

Geofence warrants deprive citizens of the ability to protect their own privacy. There is no reasonable way for a person to opt-out of having their location tracked. A person’s only choice is to completely turn off all location services, beacons, and other preferences, which is no choice at all in the modern era. Doing so would prevent the use of a phone’s critical features and applications and would defeat the purpose of possessing one. Moreover, users have been misled about the ability to opt-out of having their location history tracked by Google.¹⁶ Google records a person’s location even when the

¹¹ Alfred Ng, *Geofence Warrants: How Police can use Protesters’ Phones Against Them*, CNET (June 16, 2020) (<https://www.cnet.com/news/geofence-warrants-how-police-can-use-protesters-phones-against-them/>) (last accessed December 27, 2021).

¹² Thomas Brewster, *Google Hands Feds 1,500 Locations in Unprecedented ‘Geofence’ Search*, FORBES (December 11, 2020) (<https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/>) (last accessed December 27, 2021).

¹³ Thomas Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched A Sexual Assault Victim’s Name, Address Or Telephone Number*, FORBES (October 4, 2021) (<https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/>) (last accessed December 27, 2021).

¹⁴ Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them*, MPR NEWS (February 7, 2019) (<https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants>) (last accessed December 27, 2021).

¹⁵ Tim Cushing, *Accidentally Unsealed Documents Shows Feds Are Using Reverse Warrants to Demand Info on Google Searches*, TECHDIRT (October 7, 2021) (<https://www.techdirt.com/articles/20211005/17271147709/accidentally-unsealed-document-shows-feds-are-using-reverse-warrants-to-demand-info-google-searches.shtml>) (last accessed December 27, 2021).

¹⁶ Ryan Nakashima, *Google tracks your movements, like it or not*, ASSOCIATED PRESS (August 13, 2018) (<https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb>) (last accessed December 27, 2021).

user actively opts out: some services on Android and iPhone automatically store a person's movements even after changing the location history setting.¹⁷

Geofence searches lead to a higher rate of false positives than other location-based data. When so many devices are swept into this dragnet, law enforcement can *always* find some device that fits its narrative. Already, in the brief time that law enforcement has utilized this broad and unfettered search, there are stories of innocent individuals becoming embroiled in the criminal justice system, accused of crimes, incarcerated, and later exonerated.

For example, in January of 2020, Zachary McKoy, became a suspect in a burglary simply because his device had passed the incident location three times the day of the incident. The crime scene was on Mr. McKoy's route to and from his work and home.¹⁸ In 2018, a warehouse worker, Jorge Molina, was arrested and incarcerated for a week as a suspect in a drive-by homicide based on data tracking his device to the location where the shooting occurred. Additional investigation quickly pointed to another suspect and lead to Mr. Molina's exoneration, but not before he spent a week in jail, lost his job, and faced significant collateral consequences.¹⁹

The Legislature should act to prevent New Yorkers from falling victim to what happened to Zachary McKoy and Jorge Molina. Use of geofence searches in densely populated urban areas, poses an immediate risk to innocent New Yorkers who may be falsely identified as suspects simply because they passed through a location. The probability of wrongful accusations and the terrifying consequences that come with them are not only likely, they are inevitable.

Reverse Location and Reverse Keyword Search Court Orders Stifle New Yorkers' First Amendment Rights to Freedom of Assembly and Freedom of Speech

At a time of extraordinary upheaval and historic political participation, the right to assemble and the right to freedom of speech is ever more crucial. Across the nation and the state, law enforcement has repeatedly engaged in brutal crackdowns of activists during gatherings and protests, and employed a pattern of surveillance of communities and individuals, based on their purported political associations. The New York City

¹⁷ *Id.*

¹⁸“If you're innocent, that doesn't mean you can't be in the wrong place at the wrong time, like going on a bike ride in which your GPS puts you in a position where police suspect you of a crime you didn't commit.” Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him A Suspect*, NBC NEWS (March 7, 2020) (<https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761>) (last accessed December 27, 2021).

¹⁹ Valentino-DeVries, *supra*.

Police Department has a distinctly troubling record of targeting and surveilling activists, from the oft cited *Handschu* decree, to more recent use of biometric surveillance to identify and harass community activists.²⁰

The ease with which reverse location information and keyword searches can be used to target individuals for political activity cannot be overstated. One need not imagine a situation where law enforcement obtains location information tracking any and every device in a particular location during a rally, demonstration, protest, convention, or speech, because those situations have already come to pass. Law enforcement agencies already surveil individual's social media use, based on subjective and unfounded characterizations of members of political movements.²¹ Reverse keyword warrants similarly target and sweep up anyone searching a term out of nothing more than idle curiosity.

In 2019, the Manhattan District Attorney's Office obtained a reverse location warrant as part of an investigation of a fight occurring outside the Metropolitan Republican Club involving pro-Trump supporters known as the "Proud Boys."²² Disturbingly, the warrant obtained was not intended to help identify the *perpetrators* of the crime, but rather *everyone present, including victims who wished to remain anonymous*. The DA's Office used the warrant to further identify those victims as counter-protesters, allegedly associated with antifa, thereby targeting them entirely for their political affiliation and presence at a political gathering.²³

Similarly, leaked documents revealed one law enforcement agency's reverse keyword warrant requested information on anyone within an entire city limit who searched a particular fraud victim's name across the span of an entire year.²⁴

²⁰ See *Handschu v. Special Services. Div.*, 605 F. Supp. 1384 (S.D.N.Y 1985); Liam Stack, Annie Correal, and Juliana Kim, *N.Y.P.D. Besieges a Protest Leader as He Broadcasts Live*, NY TIMES (August 9, 2020) (<https://www.nytimes.com/2020/08/07/nyregion/nypd-derrick-ingram-protester.html>) (last accessed December 27, 2021); Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, GOTHAMIST (August 14, 2020) (<https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment>) (last accessed December 27, 2021).

²¹ Mary Pat Dwyer, & José Guillermo Gutiérrez, *Documents Reveal LAPD Collected Millions of Tweets from Users Nationwide*, Brennan Center (December 15, 2021) (<https://www.brennancenter.org/our-work/analysis-opinion/documents-reveal-lapd-collected-millions-tweets-users-nationwide>) (last accessed December 27, 2021).

²² George Joseph, *Manhattan DA Got Innocent People's Google Phone Data Through A 'Reverse Location' Search Warrant*, GOTHAMIST (August 12, 2019) (<https://gothamist.com/news/manhattan-da-got-innocent-peoples-google-phone-data-through-a-reverse-location-search-warrant>) (last accessed December 27, 2021).

²³ *Id.*

²⁴ Thomas Brewster, *Cops Demand Google Data On Anyone Who Searched A Person's Name...Across a Whole City*, FORBES (May 17, 2017) (<https://www.forbes.com/sites/thomasbrewster/2017/03/17/google-government-data-grab-in-edina-fraud-investigation/>) (Last accessed December 27, 2021).

Courts have abdicated their responsibility to meaningfully scrutinize reverse warrant applications, giving officers free range to gather data on activists at locations, even for minor incidents. There are no regulations governing law enforcement's management of the data, no information regarding the quality or quantity of seized data, and no information regarding law enforcement's use of the data once it is seized. There is absolutely no transparency, and no publicly available information regarding the government's use of reverse keyword searches. But even greater transparency cannot cure what are clearly unconstitutional searches that violate the privacy rights of innocent New Yorkers.

Conclusion: A84-A / S296-A is Necessary Legislation

A84-A / S296-A must be passed to protect the privacy rights of New Yorkers from broad unconstitutional reverse location ("geofence") and reverse keyword searches. The Legal Aid Society supports this bill and encourages the Legislature to pass it.