Brooklyn Defenders

Brooklyn Defender Services
177 Livingston St, 7th Fl
Brooklyn, NY 11201

Tel (718) 254-0700
Fax (718) 254-0897
info@bds.org

Memorandum of Support

Reverse Location and Keyword Warrant Ban

A.84 (Quart)/S.296 (Myrie)

April 2022

Brooklyn Defender Services writes in strong support of A.84/S.296, to prohibit the use of reverse location and reverse keyword searches.

BDS is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. For over 25 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality. We represent approximately 25,000 people each year who are accused of a crime, facing loss of liberty, their home, their children, or deportation. Our staff consists of specialized attorneys, social workers, investigators, paralegals, and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with educational needs of our clients or their children, housing, and benefits advocacy, as well as immigration advice and representation.

In addition to zealous legal defense, BDS provides a wide range of services to address the causes and consequences of legal system involvement. Over the last decades, we have witnessed firsthand the dramatic expansion of surveillance techniques, technologies, and systems in our city. In response, BDS established a dedicated Science & Surveillance project, which remains abreast of and responds to developments and issues of data, science, and technology in the various systems ensnaring our clients and communities.

Mass Surveillance Conducted Under the Guise of a Warrant

One such troubling development has been the rise of reverse location and reverse keyword searches: mass surveillance conducted under the guise of a warrant. Reverse location and reverse keyword warrants result in the exposure of hundreds of thousands of people's private information to law enforcement, not because they are suspected of any wrongdoing, but merely because they were in a certain area at a particular time or because they entered certain keywords into a search engine. Such searches throw a dragnet over large swaths of unknown people merely because their digitally generated data match the limitless parameters of the warrant. These fishing expeditions invade our privacy by

exploiting the enormous data collections occurring through our ever-expanding array of digital devices.

Along with a plethora of other data-aggregating and -retaining technologies, reverse location and reverse keyword warrants contribute to the creeping spread of a vast and interconnected web of surveillance that is impacting not only those caught up in enforcement systems, but also their families, communities, and advocates. This web of surveillance—driven by an unchecked appetite for access to troves of historical data—is impacting Black and brown communities at a staggering rate. The historical deployment of surveillance technologies--from simple cameras to ShotSpotter sensors, mobile license plate readers to social media surveillance--reflects law enforcement's targeting of Black and brown communities.[1] Reverse location and reverse keyword warrants represent a particularly pernicious and invasive thread of this broader web. Cell tower coverage is typically strongest in densely populated neighborhoods, which as data clearly reflects, are more likely to be historically Black and brown and among those with the highest poverty rates.

Phones and other connected devices are omnipresent in our daily lives. And while technology has advanced exponentially, state, and federal privacy laws remain largely unchanged and unresponsive. People should not have to choose between using new technologies and services or keeping their personal and digital lives out of the hands of police. The same constitutional protections that prevent police from rifling through our drawers without probable cause must also be given their full effect in protecting digital data that reveals who we are, where we go, who we know, and what we do. Law enforcement searches must be narrowly targeted, specific, and based on probable cause; reverse warrants are none of these.

Already, reverse warrants have led to multiple alarming incidents including false arrests, and they were used at First Amendment-protected protests against police brutality, ensnaring protesters in Minneapolis, Minnesota and Kenosha, Wisconsin. They are also rapidly spreading; recent disclosures by Google show a twelvefold increase of reverse location requests from 2018 to 2020, totaling 20,932 requests.

A.84/S.296 will modernize New York's privacy laws by outlawing these types of dragnet searches. Brooklyn Defender Services urges the New York State Legislature to pass A.84/S.296, so that New York's privacy laws reflect our modern digital age.

If you have further questions, please contact Elizabeth Daniel Vasquez, Director, Science & Surveillance Project at evasquez@bds.org.

[1] Barton Gellman and Sam Adler-Bell, *The Disparate Impact of Surveillance*, The Century Foundation (Dec. 21, 2017) at https://tcf.org/content/report/disparate-impact-surveillance/?session=1.