ACLU Minnesota

Reverse Warrants Testimony
Legislative Data Practices Commission

Hello House and Senate Members of the Data Practices Commission. My name is Munira Mohamed, Policy Associate for the American Civil Liberties Union of Minnesota. We're here today in support of Rep Feist's bill to ban reverse warrants.

Thank you for making time to discuss this crucial issue that poses an ongoing threat to Minnesotans' constitutional rights. Reverse warrants – also referred to as "location" or "keyword" warrants – are a perversion of the warrant system, involving significant invasions of privacy that are constitutionally suspect. These dragnet surveillances:

- Enable law enforcement to search a wide area and indiscriminately surveil large groups of people. This is done using cell phone data, GPS chips, Wi-Fi networks and Bluetooth signals.
- Can compel tech companies like Google to give up our records and release data on individuals who search for specific words or websites in a search engine.

I said this was a perversion of the warrant system because warrants are supposed to be very specific, narrowly-targeted and based on probable cause. These reverse warrants flip that requirement and become a fishing expedition, where law enforcement first searches the data then looks for probable cause in what has been collected. They allow surveillance of large groups of people over vast periods of time. It is horrifying that if police think you could have been involved in a crime, they can see what you've searched online and when you've been in specific locations.

It is easy to see the unconditional, broad nature of these warrants. That broad scope will often make investigations more difficult. Police are searching for the proverbial needle in a haystack - with the haystack getting bigger every time they use a reverse warrant. I want to contextualize this by noting how intimate the data being gathered is—we're

talking information about our health conditions, finances, sexual orientation, religious beliefs and more.

I want to draw attention to two stories: The first is a local story covered by Tony Webster[1] for MPR News. Webster reported that in 2019, Eden Prairie Police surveilled tens of thousands of people using a reverse warrant. Police collected data from Google within a dense urban area using both a 6 hour and a 33 hour window. That warrant swept in anyone who just passed through the busy area–countless random people who live, work or even just drove past.

In the end, police identified the suspects accused of burglary using other investigative techniques without Google's data, yet their invasion of the privacy of innocent individuals remains. The story also illustrates how judges – who are supposed to act as a firewall – often aren't given proper information or clarity about what they are signing off on.
The second story is about an investigative report by the ACLU of Northern California[2].

In the report, the ACLU of Northern California analyzed thousands of warrants from January 2018 to August 2021. The results of their investigation showed the shocking scale of these reverse warrants, which included 121 homes, 82 apartments, 32 bars and restaurants, 12 places of worship, seven schools and daycares, and seven medical care sites. One warrant they looked at had an error that led to the capturing data from a 2-mile stretch of San Francisco, including a United Nations building, a Courthouse, and Senior Center. This highlights the troubling issue that reverse warrants are not error proof and are ultimately a dragnet surveillance tool.

Overall, reverse warrants are fishing expeditions where everyone is guilty until proven innocent and surveilled as suspects of a crime they haven't committed. As digital technology becomes omnipresent in our everyday lives, we must protect the constitutional and privacy rights of Minnesotans.

Thank you and please consider supporting Rep Feist's much needed bill.

---

[1] https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants
[2] https://www.aclunorcal.org/news/cops-blanketed-san-francisco-geofence-warrants-google-was-right-protect-peoples-privacy/