‘Keyword Warrants’ Make Every Search A Risk

Albert Fox Cahn 2020-10-15T19:37:41

How many times did you search google today? Few of us know the answer. It’s not just the queries entered into the ubiquitous google search bars, but the countless other apps in the Google ecosystem, constantly harvesting our every question to refine their picture of even the most intimate spheres of our life. In the hands of advertisers, this technology is creepy. But when it is fully exploited by law enforcement agencies, it can be a profound danger to civil society and human rights.

Police have used search records in criminal cases for decades, but increasingly invasive and expansive types of search will further commandeer the power global tech giants as tools of government surveillance. A newly-documented trend comes in the form of keyword search warrants, which exponentially expand the power of this tracking tool.

From Investigating Individuals to Investigating Whole Communities

Historically, courts ordered Google and other search firms to divulge a defendant’s search history and location data. That type of search can be quite invasive, but it fits the broader framework for legal investigations: A person is suspected of a crime, records are held on them by a business, and that business is compelled to hand them over. But keyword search warrants reverse this process, raising alarming threats to personal privacy.

With a keyword search, police demand a list of every single user who has searched for a specific search term or “keyword.” Rather than returning information for a single person suspected of a crime, keyword warrants provide information on hundreds, thousands, or even millions of users, even though the vast majority of those identified will likely be completely innocent. Even worse, the judges who sign these orders do not know how many users will be caught up in the search at the time they approve them. They cannot because it is the keyword search itself that tells police how many individuals searched for a specific name, address, or product.

Trial court magistrates have already approved these invasive searches, but many hope they will be found unconstitutional by higher courts. Notably, keyword search warrants fail the particularity requirement found in the U.S. Constitution’s Fourth Amendment. This is because police cannot particularly describe probable cause for treating each google user who searched for an address as a suspect. Quite the opposite, they know that the vast majority of people who make such searches will have no connection to the crime

The results are chilling. Keyword warrants enable police to identify all users in a physical area, giving them a powerful tool to track members of a protest or religious community, or even those receiving reproductive medical care, including abortions.

“Hey Google, who searched for this address?”

The highest profile example of a keyword search warrant happened this past Summer, though the facts of the search are only coming to light now. The search was connected to the ongoing prosecution of the singer and accused sex offender R. Kelly, as police tried to prove one of the singer’s associates engaged in arson and witness intimidation.

In a warrant application from July 13th, a federal immigration agent detailed the prior steps that agents had taken in the investigation into R. Kelly’s associate. One seemingly innocuous line in the tediously dry 13 document held the bombshell revelation: “On June 15, 2020, the Honorable Ramon E. Reyes, Jr., United States Magistrate Judge for the Eastern District of New York, authorized a search warrant to Google for users who had searched the address of the Residence close to the time of the arson.”

Notably, in this case, the defendant wasn’t the only one to search for the address in question. No, the agent notes that the individual was merely “among the individuals who searched the address.” But the agent does not tell the court how many people made this search, whether it was dozens, hundreds, or more. Also, the agent never says what is meant by searches “close in time to the arson.” Does that mean within minutes, the same day, or just the same month?

These details are crucial, because if investigators cast a wide enough net, they can always find someone who appears to fit their theory of the case. And when they do, they simply walk up the ladder of surveillance, gathering ever more information. Here, agents used the keyword search warrant to get an order for historical cell-site information, which is able to provide a near-constant log of a suspect’s movements. As with any invasion of civil rights, this can result in positive outcomes in isolated cases, but it does not take much imagination to see how the technique can be abused.

In this way, the danger of keyword search warrants is two-fold: first these tools track large numbers of individuals with no connection to a crime, and, second, the near-limitless pool of data increases the risk of false-positives, apparent suspects who face even more invasive secondary surveillance as a result of fitting police’s anticipated pattern.

Both of these practices would have been an anathema to the framers of the American Constitution, who draft the Fourth Amendment as its particularity requirement in response to the general warrants of the colonial era. Prior to the revolution, British officials would use these general warrants to search any place, seize any person or property they sought, with almost no redress at all.

Reverse Search Warrants as a Trend

And keyword search warrants are just one of a growing list of so-called “reverse search warrants,” which upend the traditional logic of warrants and search a broad pool of innocent individuals in the hopes of finding one who is guilty.

Another chilling example is “geofence warrants,” which allow police to demand the identity of every google user in a specific area at a specific time. But geofence warrants need not be all that specific, covering a house, a neighborhood, or even an entire city. As with keyword warrant, one court order can easily cover records for thousands of users, with no way for judges to know at the time they sign the order just how many users’ data will be divulged.

Another example comes from the increasingly wide array of home DNA testing services. Websites like Ancestry.com and GEDMatch offer users the chance to explore their genealogy, to find lost relatives, and, now, to end up in a perpetual genetic lineup. GEDmatch confirmed last year that it had received at least one warrant to search its database, and Ancestry.com has actively fought off warrants as well. Much like geofence and keyword searches, these warrants force companies to search records of millions of people, all (or nearly all) are completely innocent, in the hopes of finding one potential suspect.

If the President sought to compel every American to submit to a national DNA registry, it would be completely illegal. But, using these sorts of reverse search warrants, police can effectively create the exact same tool. Certainly, not every American has participated with these home DNA tests, but they don’t have to. That’s because even if you never submit your information to one of these databases, simply having one distant relative in the database can be enough to expose your own genetic information.

Growing Legislative and Judicial Resistance

Thankfully, this trend of ever-expanding reverse search warrants hasn’t gone unchecked. Increasingly, we see pushback from trial judges and magistrates who reject requests for broad geofence warrants: “if the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials rummage where they please in order to see what turns up… a federal court in the United States of America should not permit the intrusion.”

And as the issue works its way through the court system, there is hope that appellate courts and the Supreme Court may ban the practice categorically. Similarly, there are efforts to outlaw the practice at the state level. A bill our organization, S.T.O.P., helped author is currently pending before the New York State legislature. If passed, it would outlaw all geofence warrants throughout the state.

Sadly, the pushback is piecemeal. For example, the legislation on geofence warrants wouldn’t apply to keyword warrants like those used in the R. Kelly case. The reason why: we didn’t know this type of search was taking place. In this way, we see the constant constitutional catch up for those pushing back against new search tools in the United States. In the absence of a more fundamental shift in Constitutional

jurisprudence or unpresented privacy legislation, police will continue to have a free hand to concoct ever more invasive ways to harvest our digital data, operating with a free hand as lawmakers and the public struggle to keep up.
