

## Police Use Contact Tracing and Big Tech to Identify Protesters

By MassPrivatel

Global Research, June 05, 2020

MassPrivatel 2 June 2020

Region: <u>USA</u>

Theme: Intelligence, Law and Justice,

Police State & Civil Rights

Countless warnings about how law enforcement could use contact-tracing apps to monitor people have gone unheeded.

As BGR.com revealed police are using contact tracing to identify protester's affiliations.

"According to Minnesota Public Safety Commissioner John Harringon, officials there have been using what they describe, without going into much detail, as contact-tracing in order to build out a picture of protestor affiliations — a process that officials in the state say has led them to conclude that much of the protest activity there is being fueled by people from outside coming in."

A Twitter feed titled <u>"Minnesota Contact Tracing"</u> revealed how police are using contact tracing to identify and arrest protesters. "Minnesota Public Safety Commissioner John Harrington says they've begun contact tracing arrestees."

Recently, 100 human rights groups <u>warned</u> that an Apple-Google contact tracing app could be used as a cover to identify activists and minorities.

"An increase in state digital surveillance powers, such as obtaining access to mobile phone location data, threatens privacy, freedom of expression and freedom of association, in ways that could violate rights and degrade trust in public authorities—undermining the effectiveness of any public health response. Such measures also pose a risk of discrimination and may disproportionately harm already marginalized communities."

So despite all assurances to the contrary, it appears that 100 human rights groups were right; law enforcement can and will use contact tracing to identify protesters.

Updated 6/3:

VoteMap used anonymous data to identify protesters phones

According to an <u>article</u> in *The Detroit News*, police can identify anonymous protesters cell phones.

"The tracking, known as geoharvesting, is when data is gathered from a smartphone app on a device connected to the internet. That data contains geolocation information that can be queried to show movement on a map."

"The cellphone users remained anonymous and their locations were instead culled from the publishers of the opt-in apps they were using, said McEwan, CEO of the Austin-based startup Datum that is the parent company under which VoteMap falls. People gauging cellphone locations the day of the April 30 protest and the day after would not be able to see to whom the phone belonged," she said. (To find out more about VoteMap click here.)

As NBC News <u>noted</u>, contact tracers also use geofencing to help identify protesters.

"Geofencing" captures the social media posts of people entering a specific area. The technology locates any cellphones that cross into the area by locking onto their geolocation systems, and then records social media posts and sometimes other data from the phones."

Time <u>exposed</u> how the military (National Guard) uses a classified system called "Secret Internet Protocol Router" or SIPR to monitor protesters. (To learn about Perspecta Inc.'s role click here & here.)

Big Tech's hands are dirty with Federal money paying for new ways to monitor Americans.

A recent *Business Insider* <u>article</u> describes how police use Big Tech to monitor activists and protesters the moment they walk out their door.

"Law enforcement agencies have made full use of high-tech surveillance tools as protests sweep the country following the death of George Floyd. A predator drone operated by Customs and Border Patrol circled above protesters in Minneapolis."

Buzzfeed News warns, "law enforcement has a wide breadth of surveillance technologies that could be used to monitor and target protesters — including controversial facial recognition software Clearview AI, license plate readers, body cameras, and video analysis tools."

Both of these articles reveal a frightening array of Big Tech surveillance devices being used by police nationwide.

Minneapolis police and the Minnesota Fusion Center are also using Clearview AI, BriefCam, Ring doorbell cameras, Axon police body cameras, ShotSpotter and license plate readers to create an intimate view of people's lives.

BuzzFeed's article also revealed how police use Arxys "Milestone" software which uses video detection and analytics to identify people.

"The Minneapolis Police Department said in a <u>surveillance white paper</u> that it uses <u>Arxys [Milestone] software</u> — a video management tool that claims to offer "video motion detection" and "video analytics" — to analyze CCTV footage."

While both articles do a great job of revealing some of the ways law enforcement can monitor anyone, it really did not go into detail about how invasive Big Tech's surveillance devices truly are.

Let's say you use your smartphone for everything; texts, phone calls, pictures, music, etc., if you also use Alexa or a NEST thermostat or any smart device in your home, these devices collect, store and transmit all that personal data, which police can use to identify a person. Police can also identify people who use a Tablet or laptop, because like a phone they have an IP and MAC address.

If you use any of these devices to make online purchases, police can ask those companies to provide details of what you bought and when. Anytime you use a credit/debit or customer rewards card, someone is compiling a database of everything you purchased.

Let's say you drive or take public transit, police can track your vehicle and they can use facial recognition to identify where you work or which bus or train stops you use.

If you drive or take an Uber or Lyft, chances are your personal information is being recorded and used to build a massive database of your comings and goings. From the moment you step outside of your home, your neighbor's Ring doorbell or Flock cameras have identified you, your family and your vehicle.

And if they are any social distance snitches in your neighborhood, they have recorded you and reported you to police via Ring Neighbors or NextDoor.

Thanks to Big Tech, a person's everyday life is no longer private. Now everything we do is being recorded in real-time. Things like what and where you eat, who your friends and family members are, who your family doctor is or where you worship are all available to law enforcement.

Despite what Big tech, politicians and law enforcement say, AI and smart devices are being used to identify activists and protesters.

\*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Featured image is from Study.com

The original source of this article is <u>MassPrivatel</u> Copyright © <u>MassPrivatel</u>, <u>MassPrivatel</u>, 2020

## **Comment on Global Research Articles on our Facebook page**

## **Become a Member of Global Research**

Articles by: MassPrivatel

**Disclaimer:** The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: <a href="mailto:publications@globalresearch.ca">publications@globalresearch.ca</a>

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: <a href="mailto:publications@globalresearch.ca">publications@globalresearch.ca</a>