Governments Haven't Shown Location Surveillance Would Help Contain COVID-19

Governments around the world are demanding new dragnet location surveillance powers to contain the COVID-19 outbreak. But before the public allows their governments to implement such systems, governments must explain to the public how these systems would be effective in stopping the spread of COVID-19. There's no questioning the need for far-reaching public health measures to meet this urgent challenge, but those measures must be scientifically rigorous, and based on the expertise of public health professionals.

Governments have not yet met that standard, nor even shown that extraordinary location surveillance powers would make a significant contribution to containing COVID-19. Unless they can, there's no justification for their intrusions on privacy and free speech, or the disparate impact these intrusions would have on vulnerable groups. Indeed, governments have not even been transparent about their plans and rationales.

The Costs of Location Surveillance

EFF has long opposed location surveillance programs that can turn our lives into open books for scrutiny by police, surveillance-based advertisers, identity thieves, and stalkers. Many sensitive inferences can be drawn from a visit to a health center, a criminal defense lawyer, an immigration clinic, or a protest planning meeting.

Moreover, fear of surveillance chills and deters free speech and association. And all too often, surveillance disparately burdens people of color. What's more, whatever personal data is collected by government can be misused by its

employees, stolen by criminals and foreign governments, and unpredictably redirected by agency leaders to harmful new uses.

Emerging Dragnet Location Surveillance

China reportedly responded to the COVID-19 crisis by building new infrastructures to track the movements of massive numbers of identifiable people. Israel tapped into a vast trove of cellphone location data to identify people who came into close contact with known virus carriers. That nation has sent quarantine orders based on this surveillance. About a dozen countries are reportedly testing a spy tool built by NSO Group that uses huge volumes of cellphone location data to match the location of infected people to other people in their vicinity (NSO's plan is to not share a match with the government absent such a person's consent).

In the United States, the federal government is reportedly seeking, from mobile app companies like Facebook and Google, large volumes of location data that is de-identified (that is, after removal of information that identifies particular people) and aggregated (that is, after combining data about multiple people). According to industry executives, such data might be used to predict the next virus hotspot. Facebook has previously made data like this available to track population movements during natural disasters.

But re-identification of de-identified data is a constant infosec threat. De-identification of location data is especially hard, since location data points serve as identification of their own. Also, re-identification can be achieved by correlating de-identified data with other publicly available data like voter rolls, and with the oceans of information about identifiable people that are sold by data brokers. While de-identification might in some cases reduce privacy risks, this depends on many factors that have not yet been publicly addressed, such as careful selection of what data to aggregate, and the minimum thresholds for aggregation. In the words of Prof. Matt Blaze, a specialist in computer science and privacy:

> One of the things we have learned over time is that something that seems anonymous, more often than not, is not anonymous, even if it's designed with the best intentions.

Disturbingly, most of the public information about government's emerging location surveillance programs comes from anonymous sources, and not official explanations. Transparency is a cornerstone of democratic governance, especially

now, in the midst of a public health crisis. If the government is considering such new surveillance programs, it must publicly explain exactly what it is planning, why this would help, and what rules would apply. History shows that when government builds new surveillance programs in secret, these programs quickly lead to unjustified privacy abuses. That's one reason EFF has long demanded transparent democratic control over whether government agencies may deploy new surveillance technology.

Governments Must Show Their Work

Because new government dragnet location surveillance powers are such a menace to our digital rights, governments should not be granted these powers unless they can show the public how these powers would actually help, in a significant manner, to contain COVID-19. Even if governments could show such efficacy, we would still need to balance the benefit of the government's use of these powers against the substantial cost to our privacy, speech, and equality of opportunity. And even if this balancing justified government's use of these powers, we would still need safeguards, limits, auditing, and accountability measures. In short, new surveillance powers must always be necessary and proportionate.

But today, we can't balance those interests or enumerate necessary safeguards, because governments have not shown how the proposed new dragnet location surveillance powers could help contain COVID-19. The following are some of the points we have not seen the government publicly address.

1. Are the location records sought sufficiently granular to show whether two people were within transmittal distance of each other? In many cases, we question whether such data will actually be useful to healthcare professionals.

This may seem paradoxical. After all, location data is sufficiently precise for law enforcement to place suspects at the scene of a crime, and for juries to convict largely on the basis of that evidence. But when it comes to tracking the spread of a disease that requires close personal contact, data generated by current technology generally can't reliably tell us whether two people were closer than the CDC-recommended radius of six feet for social distancing.

For example, cell site location information (CSLI)—the records generated by mobile carriers based on which cell towers a phone connects to and when—is often only able to place a phone within a zone of half a mile to two miles in urban areas. The area is even wider in areas with less dense tower placement. GPS sensors built directly into phones can do much better, but even GPS is only

accurate to a 16-foot radius. These and other technologies like Bluetooth can be combined for better accuracy, but there's no guarantee that a given phone can be located with six-foot precision at a given time.

2. Do the cellphone location records identify a sufficiently large and representative portion of the overall population? Even today, not everyone has a cellphone, and some people do not regularly carry their phones or connect them to a cellular network. The population that carries a networked phone at all times is not representative of the overall population; for example, people without phones skew towards lower-income people and older people.

3. Has the virus already spread so broadly that contact tracing is no longer a significant way to reduce transmission? If community transmission is commonplace, contact tracing may become impractical or divert resources from more effective containment methods.

There might be scenarios other than precise, person-to-person contact tracing where location data could be useful. We've heard it suggested, for example, that this data could be used to track future flare-ups of the virus by observing general patterns of people's movements in a given area. But even when transmission is less common, widespread testing may be more effective at containment, as may be happening in South Korea.

4. Will health-based surveillance deter people from seeking health care? Already, there are reports that people subject to COVID-based location tracking are altering their movements to avoid embarrassing revelations. If a positive test result will lead to enhanced location surveillance, some people may avoid testing.

Conclusion

As our society struggles with COVID-19, far narrower "big data" surveillance proposals may emerge. Perhaps public health professionals will show that such proposals are necessary and proportionate. If so, EFF would seek safeguards, including mandatory expiration when the health crisis ends, independent supervision, strict anti-discrimination rules, auditing for efficacy and misuse, and due process for affected people.

But for now, government has not shown that new dragnet location surveillance powers would significantly help to contain COVID-19. It is the government's job

to show the public why this would work.

JOIN EFF LISTS

Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

SUBMIT

RELATED UPDATES

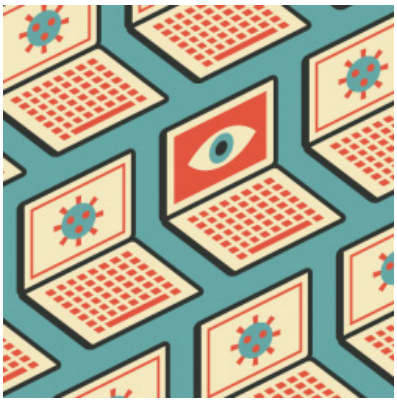
DEEPLINKS BLOG BY ERNESTO FALCON | MARCH 23, 2020

Social Distancing, The Digital Divide, and Fixing This Going Forward

The California Public Records Act Is an

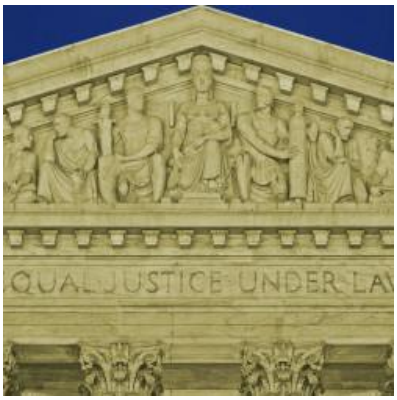
DEEPLINKS BLOG BY DAVE MAASS | MARCH 23, 2020

Essential Right, Even During a State of Emergency



DEEPLINKS BLOG BY CINDY COHN | MARCH 23, 2020

EFF and COVID-19: Protecting Openness, Security, and Civil Liberties



DEEPLINKS BLOG BY NAOMI GILENS, ALEX MOSS | MARCH 23, 2020

The Time Is Now: The Supreme Court Must Allow Live Cameras

Embracing Open Science in a Medical Crisis

DEEPLINKS BLOG BY RORY MIR | MARCH 20, 2020

DEEPLINKS BLOG BY JASON KELLEY | MARCH 20, 2020

Governments Must Commit to Transparency During COVID-19 Crisis

DEEPLINKS BLOG BY MATTHEW GUARIGLIA | MARCH 19, 2020

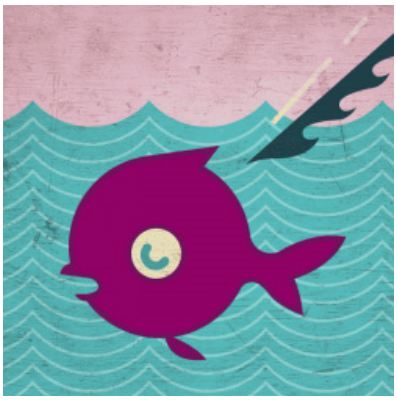
Face Surveillance Is Not the Solution to the COVID-19 Crisis

Right to Repair in Times of Pandemic

DEEPLINKS BLOG BY CORY DOCTOROW | MARCH 19, 2020

DEEPLINKS BLOG BY LINDSAY OLIVER | MARCH 19, 2020

What You Should Know About Online Tools During the COVID-19 Crisis



DEEPLINKS BLOG BY DALY BARNETT, SORAYA OKUDA | MARCH 19, 2020

Phishing in the Time of COVID-19: How to Recognize Malicious Coronavirus Phishing Scams