GlobalResearch
Center for Research on Globalization

COVID-19 Contact Tracing and State Surveillance

By Tracy Rosenberg and Ann Garrison
Global Research, January 07, 2021

Region: USA
Theme: Intelligence, Police State & Civil Rights

The US remains wholly incapable of tracing Covid-19 contagion, but if it tried, we might wind up with "the worst of both worlds" – a horror of coercion and confusion that still failed to stop the epidemic.

> "Low income communities, particularly Black and Brown communities, have reasonable fears that at least some law enforcement agencies might use access to contact tracing data to harass them."

*I spoke to Bay Area privacy activist **Tracy Rosenberg** about the danger that data contact tracing to track the spread of COVID-19 will become available to the surveillance state.*

***

Ann Garrison: Many fear that digital contact tracing to stop the spread of COVID-19 will expand surveillance states' ability to curtail privacy and control their populations. Can you explain what contact tracing is?

Tracy Rosenberg: Contact tracing is the process of creating a map of a person's movements and associations in order to identify the possible spread of infectious disease. Before the age of digital technology, it was an onerous process of paper surveys, which while they contained very personal information, had some practical limitations on any additional use. In the age of digital technology, the ability to retain, repurpose and search large data chains is greater than it has ever been in human history. Contact tracing data, when performed by government public health agencies, is medical health data and is protected by the same laws that protect other health data.

AG: What dangers does it pose?

TR: Well, there are quite a few. One is emergency protocols. A large tracing program set up under emergency conditions can often lead to incomplete frameworks and poorly trained personnel, including some with relatively little or no familiarity with health data protections. When data protections, storage and access protocols are not well-planned, leaks, hacks and unauthorized access sometimes occur.

AG: Can you describe what a well-planned data protection plan would be? Who would have access to what and who not, and how would we know that the FBI, CIA, NSA, and Mossad hadn't gotten into it?

TR: It's not an easy question, but generally data protection requires retention limits (i.e., only keeping things for as long as you actually need them and no longer), disaggregating

bulk data from personally identifying information as soon as possible, clear demarcations of access by job title, several layers of anti-hacking security protections, clear consent procedures, and training. An emergency like a pandemic is always the enemy of planned data protections. But there have been efforts.

For example, California privacy groups tried to pass protective legislation in 2020 for contact tracing software (AB 1782 and AB 660) that among other things would have established procedures for providing and revoking consent, required at least some level of encryption for stored data, required public reports and metrics every 90 days, and prevented law enforcement agencies from participating in or having access to contact tracing data. (That's a broad summary, but it gives you the idea.) Sadly, both bills were vetoed by Gavin Newsom who argued that he did not want regulations that might slow down contact tracing efforts in the state.

It's a habitual trend in American politics that we don't want to address privacy issues during emergencies, which has then led to revelations of upsetting practices after the fact. In theory, agencies like FBI, CIA, NSA, and Mossad (to use your examples) should have no access to health data that is already protected by law. But in an emergency, with a bunch of entities that are both public and private rushing in to try to help and set up new processes–that is exactly how the guard rails slip and things happen that aren't supposed to happen.

AG: Doesn't any privacy protection plan or policy depend on the good faith of those expected to follow it? This is true with any policy, but the use of Big Data seems particularly difficult to detect.

TR: Good faith only goes so far. Firstly, it probably isn't that good an idea to depend on the intentions of government agencies, which are filled with a large variety of people. While I believe most public health workers are dedicated and conscientious, one can never say anything concrete about 100% of the people involved in anything, and the nature of a pandemic is to draw in other additional agencies and entities with relatively little experience with handling large amounts of health data and personally identifying information (PII). In general, our approach to privacy regulations is that enforcement is required. A policy without enforcement protocols and consequences for violations is a recommendation. The vetoed California bills I mentioned both included private rights of actions that allow anyone to take a legal action to ensure compliance. Basically crowdsourced enforcement, which provides a step that can be taken if and when good faith is not enough.

There isn't any doubt that the use and distribution of any set of Big Data can be hard to detect in real time. The only privacy protection that is 100% bulletproof is not to collect the information in the first place. But if that's not an option (and a reasonable case can be made that it probably isn't, at least in the early stages of a pandemic), then enforceable regulations are the next best thing.

At this point in the COVID-19 pandemic in the US, case numbers are far exceeding any realistic contact tracing program, so we may have the worst of both worlds, which is half-assed and partial contact tracing with limited effect on actually reining in the pandemic and with no effective or enforceable regulations.

AG: The California Development Department has been announcing jobs for contact tracers every day since the COVID pandemic began, and employment information is readily

available on the Web. They usually include the promise that you can “work from home” and don’t require much experience. What kind of training do you think contact tracers should have?

TR: A thorough review of federal and state protections for medical data. A one-way data uplink that removes data access once it is submitted to a public health agency so it cannot be recovered and stored on a personal hard drive or shared.

AG: What about cross-state and cross-border contact tracing? How is that being handled?

TR: Best as I can tell, remarkably ad hoc and randomly. Since the federal government under Trump has largely shifted pandemic response onto the states to deal with, there is a big handicap in dealing with cross-state episodes. We’ve seen that with incidents like the MA conference that allegedly spread a great deal of virus in the early days of the pandemic as conference-goers went home all across the country, but primarily to the large urban cities, and the few attempts at national contact tracing of Florida spring break participants. Probably the most active federal involvement apart from some of the vaccines has been at the airports, but as we’ve seen it’s been pretty marginal, with random travel bans on some foreign countries at some times, and somewhat chaotic testing protocols that I’m not sure people really believe are that effective, given the limitations of PCR testing for infection.

AG: What are some of the other dangers of contact tracing?

TR: Another issue is consent. The right to agree or not agree to participate in contact tracing is an important privacy value. While very few have advocated for mandatory participation in the US, that would potentially be a privacy issue. What is more worrisome is what we call coerced participation, which is pressure from employers or social service agencies which impairs freely given consent by suggesting adverse consequences for those who do not participate. California had proposed bills in 2020 to ban retaliation against individuals who chose not to participate, but Governor Newsom vetoed those contact tracing regulatory protocols.

AG: It’s worth noting here that Governor Newsom is widely considered to be a future presidential candidate.

TR: Yes.

AG: It seems that most contact tracing is done with cell phone apps that people are downloading voluntarily, although Singapore is also deploying a wearable token. Are most people who now choose to participate in contact tracing downloading an app onto their phone?

TR: The Apple/Google Notify app is a fairly widespread mode of contact tracing. There are a lot of downloads of the app, although there is no real way to verify how many of those people have turned on Bluetooth to use the app and how many are carrying their cell phone everywhere they go. As I said, this particular app was developed to minimize privacy risks and does not collect too much PII. However, testing facilities, which are run in a lot of different ways in different states, may also be engaging in contact tracing with positive test results, and how all of that is working across the country is a bit unclear. There are also anecdotal reports of large employers engaging in some ad hoc contact tracing when their employees test positive, which of course happens in a black box.

AG: Singapore has already excluded anyone who refuses to participate in contact tracing access to public space, and openly stated that they will make data available to police to investigate crimes. That's not surprising because Singapore is one of the most tightly and openly controlled states in the world. Who is pressing for mandatory participation here?

TR: I don't think anyone has openly pushed for mandatory participation in contact tracing. If they have, I'm not aware of it. But there is concern about coerced participation with employers pressuring employees, or educational bureaucracies pressuring teachers and students that would have people fearing informal retaliation or discrimination if they prefer not to participate. In my view, mandated participation requires extensive safeguards. Laissez-faire should not operate in only one direction. If the government will not take action to safeguard my personal information, then I have a choice whether to trust them with it—or not.

AG: What's next on your list of concerns?

TR: Another is technology. As with anything else, technology can make large-scale tasks much easier, but it can also introduce more problems. Automated contact tracing programs can potentially introduce greater scale and speed, but also introduce storage and access questions that can impair data safety, sometimes in ways that are not clear until something bad happens. It bears repeating that the California Notify app, one of the first automated contact tracing programs to go forward with public distribution, was carefully designed with privacy rights in mind and, at least on paper, its protocol should prevent many of the problems that could be anticipated.

AG: Can you give us an example of "something bad happening"?

TR: A list on the dark web or even the plain old Internet of people with positive COVID tests in the last month in Philadelphia with the names and addresses of anyone they can remember having contact with, secured by a hacker. A FOIA request that comes back in 2022 with emails from FBI agents referring to "tapping into" the NY COVID database to find someone they are looking for. Vaccine passports required for bus, train, and plane travel that cannot be acquired without a social security number, which turns undocumented Americans into literal fugitives in the country they live in and turns victims of identity theft into one big no-travel list. None of these things are impossible from a badly regulated contact tracing effort.

AG: What about law enforcement access outside Singapore, where it's already acknowledged?

TR: That's of course one of the greatest concerns. First responders are sometimes seen as participants in contact tracing administration. While this can make sense on the EMS public health end, it becomes concerning when extended to police and fire. One of the restraints that California's 2020 legislation sought to establish was a red line keeping police out of contact tracing. But, as mentioned, that was vetoed by California's governor.

Communities have what I think are reasonable fears based on past experiences that at least some law enforcement agencies might use access to contact tracing data to harass low income communities, especially in Black and Brown neighborhoods or homeless people. It is definitely true that some police agencies have demonstrated ongoing violations of data-sharing limitations of all kinds, which usually come to light after the fact, so the role of law

enforcement in contact tracing is an ongoing concern.

AG: Anything else?

TR: Beyond those four specific concerns, there are always broader concerns that lists of "the exposed" or "the infected," like any government list of people (like lists of "suspected terrorists" or "antifa" or "black identity extremists"), could under certain political conditions be used to strip some level of Constitutional protections from the people on the list. This would be a secretive government activity unsanctioned by law, but it has certainly happened before in American history.

AG: Since the Snowden release about NSA surveillance, many people assume that the horse is out of the barn, that we have no privacy left, but I know you continue to work on privacy issues with multiple coalitions and at multiple levels of government. Can you explain why you still have hope and think this is worth doing?

TR: Section 215 of the Patriot Act, which more or less legalized most of the NSA's snooping, was not renewed by Congress after 20 years. That's a big deal. In reality, although an agency like the NSA has enormous access, the numbers of people they actually touch is tens of thousands in a year, while there are hundreds of millions in the US. So there is plenty of room to protect literally mountains of collected data, first by trying to reduce the size of the mountain and secondly by installing guardrails to limit abuse and misuse. It is never a question of 100% success because that won't happen, but I can say after several years that the visibility of the conversation and the acknowledgment of the risks have increased by a quantum amount from say 2013 to 2021. I do not think this pandemic emergency has (at least not yet and not in the United States) set loose the kind of mass privacy violations unleashed by 9-11. That said, it has unleashed an economic crisis and social control limitations that become increasingly debilitating the longer they drag on. And it is not wrong to say that the economic disenfranchisement of millions over the course of a year certainly can work in the interests of oppression and authoritarianism. A state of ongoing emergency is a state in which things that would never fly in a non-emergency can become institutionalized.

AG: There's a lot of concern about contact tracing expressed in mainstream outlets. What could you say about how widespread and effective the resistance to abuse of the data has been so far?

TR: With regard to the pandemic, objections to masks and social distancing as well as business closures and fears about the vaccines have been all tangled up with contact tracing worries in kind of a soup of general anxiety. It has been difficult to separate out all of the pieces into coherent public policy recommendations. So I'd say we have widespread and ineffective resistance. Probably the folks pursuing eviction moratoriums have been the most successful in getting protections actually put into place, and even those have been only partially effective. We definitely have not provided the economic support people need for a real disease-prevention lockdown, nor have we made it possible to identify everyone exposed and assist them with a real isolation period to stop any spread. Without those things, we end up with a very, very long period of emergency, which has huge risks as outlined above.

*

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.

Tracy Rosenberg *is the Executive Director of Media Alliance and a founding member of Oakland Privacy.*

Ann Garrison *is an independent journalist based in the San Francisco Bay Area. In 2014, she received the Victoire Ingabire Umuhoza Democracy and Peace Prize for promoting peace through her reporting on conflict in the African Great Lakes Region. Please help support her work on Patreon. She can be reached on Twitter @AnnGarrison and at ann(at)anngarrison(dot)com.*

Featured image is from Shutterstock

Articles by: **Tracy Rosenberg** and **Ann Garrison**