UCLA Institute for Technology, Law and Policy

Podcast Episode 7: Mohammad Tajsar of the ACLU on "Digital privacy in the age of Covid-19"

Date: April 30, 2020
Duration: 41 minutes

Biography: Mohammad Tajsar is a Staff Attorney at the ACLU of Southern California, which he joined in 2017. His work there has spanned a wide range of areas, including digital rights and government surveillance. Prior to joining the ACLU, he worked at a law firm where he focused on civil rights and workers' rights, and prior to that he was a law clerk in United States District Court for the District of Nevada and a legal fellow at the ACLU of Southern California. He has a law degree from UC Berkeley and an undergraduate degree from UCLA.

Transcript:

(Note: This transcript has been lightly edited for clarity. The transcript is presented "as is" with no representations or warranties regarding accuracy. Please consult the original audio for the definitive record of the interview.)

John Villasenor: So I'd like to give a warm welcome to Mohammad Tajsar of the ACLU, and Mohammad is a staff attorney at the ACLU of Southern California, which he joined in 2017. His work there has spanned a wide range of areas including, very importantly for today's discussion, digital rights and government surveillance. Prior to joining the ACLU, Mohammad worked at a law firm where he focused on civil rights and workers' rights, and prior to that, he was a law clerk in the United States District Court for the District of Nevada and a legal fellow at the ACLU of Southern California. He has a law degree from UC Berkeley and an undergraduate degree from UCLA. So first of all, thank you very much, Mohammad, for coming on the podcast to talk about this really important topic.

Mohammad Tajsar: Thank you, John. It's a pleasure to be here.

John Villasenor: So first question is there's been a lot of talk about potentially using data from mobile phones to combat the spread of the virus. So for example a special location tracking app could make it, at least in theory, possible to know if you've been in proximity to somebody who might be contagious. In the United States, the discussion has mostly been about doing this tracking using an app provided by private companies on an opt-in basis. So in other words, you'd only be tracked by this app if you choose to download it and then run it. What are some of the privacy concerns that you believe this would raise?

Mohammad Tajsar: Yeah, it's a great question and one that I think is on a lot of people's minds. I think before I answer that question, I think it may be useful to actually step back and provide some context and really define what it is that we're talking about here. I think most of the kind of technologically assisted tools that are being discussed to address Covid-19 fall into the broad category of contact tracing. So I'm sure people have heard this term a lot, and it bears thinking about for at least a moment to figure out exactly what contact tracing is and then to determine whether technology is appropriate as a mechanism of doing it.

Mohammad Tajsar: So what is contact tracing? It basically is a long-standing public health technique that attempts to identify everyone that a sick person may have been exposed to, and then it helps those exposed individuals identify and evaluate their risk of contracting the disease and indeed spreading it further. And then in theory it would result in some appropriate action taken in response to that information.

Mohammad Tajsar: So traditional contact tracing is typically done manually. So what that means is I go to the hospital, and I am diagnosed with a particular disease. Then somebody comes and asks me, "Hey, where have you been? This disease is infectious. We need to know the potential spread that you have caused just by living and breathing and doing what you do." And that kind of manual interview is typically conducted by humans and is often quite slow for various reasons. What then is done after that interview is a team or an individual then goes out to all of the potential other people that you have contacted, say for instance, your family members, friends, colleagues, and informs them, "Hey, Mohammad has this disease. You all might be at risk." So that's typically the universe that we're talking about here when we're talking about contact tracing.

Mohammad Tajsar: The question then becomes: Can technology make this process better? Can it make it easier, faster, more nimble, particularly when dealing with a disease that itself is incredibly infectious and fast moving? And I think the answer to that is maybe, probably not, who knows? And I think that's true for a lot of reasons, but part of the big problem with that model, there's sort of two, it seems to me. One are the privacy concerns, and one are, I think, the efficacy concerns. We're not really talking about efficacy here, but I think the efficacy of these tools depends on, not necessarily the technologies themselves, but the entire political, social, and healthcare systems that exist around the tools to be able to provide the kind of medical, health, and social assistance that people need.

Mohammad Tajsar: In other words, if you don't have functioning hospitals, it doesn't matter if we're contact tracing because you can't get the care that you need if it is determined that you are in touch with somebody that was infected. So that I think is important. That's the reason why, it seems to me, that contact

tracing, that the conversation about privacy and efficacy is one that I think is a secondary one to the principal question, which is do we have the kind of healthcare infrastructure to be able to provide at scale the kind of services that people need in order to survive this pandemic? So that's the context.

Mohammad Tajsar: The question becomes, okay, well, given the proposals that exist with respect to technically assisted contact tracing, are there downsides? Are there risks, and how useful are they? And the reality is that there are a lot of downsides, a lot of potential risks, and it's not at all clear whether these proposals can actually perform the epidemiologically necessary functions that an ordinary contact tracing scheme is design to perform. And I think that's true for a number of reasons.

Mohammad Tajsar: There are a couple that I think I'd like to address here that are important, that really the key to the success of these kinds of technically assisted contact tracing proposals that you and I can talk about a little bit further is how widely adopted they are, and wide adoption is a function of trust. How trustworthy do people in the population feel when it comes to interacting with that system? You can imagine in a manual setting, if somebody comes and interviews me and says, "Hey, you've been infected. Where have you been?" If I say, "Hey, go pound sand. I don't want to talk to you because I don't trust you," that system's not going to work. In the same way, that level of trust is necessary for a technically assisted system. If I download an app that performs this function, I need to be able to trust that that app is going to do the things that it's designed to do and not do things that are surreptitious and that are against my interests.

Mohammad Tajsar: So how then do you build trust with a technically assisted contact tracing platform? You do it in a number of different ways, and the principal way that I think you do it is by ensuring that the system is built technically from the ground up to ensure the privacy of individuals who use the system. If it is not, then you are unlikely to get the widespread adoption that's necessary for you to meet your goals, and I think that is really what's at stake here is how can you build a system that is trustworthy enough to be able to serve the goals that you want to serve? And then you can ask the question of okay, how can we configure this system in a way that mitigates some of those privacy risks? And we can if you want, John, we could talk about some of those privacy risks because I think that there are plenty, but that's the overall framework that I think is important when thinking about these systems.

John Villasenor: And yeah, could you give a couple of examples of some of the privacy risks that you are most concerned about?

Mohammad Tajsar: Sure. So first, I mentioned voluntariness, right? You can imagine privacy is a function, it seems to me, of autonomy. When we talk about privacy, what we're saying is we want to preserve the autonomy of individuals and community members and not feel like we're being coerced into providing information that we don't want to provide or doing something that we don't want to provide. So the first key principle to preserve privacy is to make sure that the system is not compulsory, that is, that you cannot force people to be a part of a system because that violates their own autonomy, and it inhibits the adoption of this system widely. So that's critical, it seems to me.

Mohammad Tajsar: Second, I think people have to own the system and own the data that is generated. So information about my own health is information that I have a control, ownership, and rights over, and it has to be the case that these systems have to allow people to make decisions about their data and not be systems that are designed to extract, either surreptitiously or otherwise, information from people. So what does that look like in practice? So for instance, if I design a system that tracks my location publicly, I need to be afforded the opportunity to turn off that location tracking as I see fit. So for instance, if I went to a friend's home to pick something up, but I was wearing fully protective gear on me, and I was quite convinced that there was no way that I would've either contracted or infected somebody else, I should have the option of telling the application or the system that I don't want to share that particular information because I'm pretty confident that I wouldn't have infected somebody. That's an example of the kind of autonomy that we're talking about.

Mohammad Tajsar: Another example might be don't share information when I'm in my own home, so turning it off at night for instance. That's the kind of control that needs to exist in a technically assisted contact tracing system that I think can preserve individual's privacy. There are a bunch of other ones, but those are good examples.

John Villasenor: Okay so, if you don't mind, let me ask you a question about the compulsory aspect. One concern is with an opt-in app for potential exposure tracking. I can imagine a scenario where in practice it becomes no longer really opt-in, and what I mean by that, if for example, many employers start saying, "You can't work here, be hired here, unless you have this app." Then in a practical sense, it really no longer becomes opt-in because it becomes a hurdle that one has to cross in order to actually earn a living. Is that a reasonable concern, and if so, how should it be addressed?

Mohammad Tajsar: Oh, absolutely. I think it's a tremendous concern. As I say, the voluntary adoption of these systems is critical to their use. So if you don't have mass adoption at scale, and then you don't have the mass healthcare

infrastructure that can respond to the information gathered by the scaled-up technology, then the system will fail. So let's assume for the moment that the system's only used by a small fraction of the population. For instance, if I use a Bluetooth-based application on my phone, there'd be no way for other people who are in contact with me who don't have that application or don't have that particular kind of technology to know that they were potentially exposed to me. So the wide-scale adoption is critical.

Mohammad Tajsar: And then if you force that kind of adoption on people, it is unlikely that they're going to trust the system and implement it and use it in a way that will give you the desired outcomes that you want to create. So then how do you do it? How do you create a system that is truly opt-in but that it gives people the trust that they need in order to really opt-in and to be comfortable with what the system is designed to do? And I think there are a number of ways you could do it. There are a number of privacy-preserving design elements that you can adopt that, for instance, retain data in an encrypted fashion, doesn't leak data, doesn't use centralized authorities to store information, doesn't maintain sensitive information like, for instance, precise location information, but instead, uses other forms of data, doesn't identify data to particular people, only keeps data as long as it's necessary, destroys it when it's no longer necessary. There's kind of a host of different privacy preservation tools that you can use to build trust.

Mohammad Tajsar: But beyond the design, then you have to also create a system that's auditable, meaning a system that uses free and open components that allows it to be reproducibly built by others to audit the system, to look through source code and the software itself to ensure that there are no leaks in the system, that there are no vulnerabilities and things like that. The system has to be auditable by experts and by everybody. In addition, you have to also sustainably develop the system, so funding all of the different categories of people and developers that create the system, ensure that they have adequate resources to be able to iterate on the design, to fix problems, make it better over time. It has to be a sustainable effort because otherwise you'll have an outdated system that has a bunch of problems that nobody fixes, and you're stuck on version 1.0 when the world has passed you by.

Mohammad Tajsar: And then I think this part is also critical. The system also has to publish benchmarks, that is, metrics to publicly demonstrate that it's being either effective or is useful to serve the goals that it wants to serve, and that I think goes a long way to ensuring trust in the system, that this is not something that's being used for nefarious ends or for something that I wasn't told about but in fact is being used in a ways that public health officials desired it to be used. So those are just some strategies designed to

obviate the problem of compulsion and create a system that is based on trust and based on voluntary participation.

John Villasenor: Well, thank you very much. So I have a question now about government. I mean the previous questions we were talking about an app, for example, created on an opt-in basis by a private entity. But suppose a government entity were to attempt to compel people to install a location tracking app that would provide this sort of data to the government. I can imagine that that would lead quite quickly to a Fourth Amendment challenge, and obviously none of us has a crystal ball, but do you think in general that a challenge like that would be likely to be successful?

Mohammad Tajsar: I'm skeptical that it would, actually to be quite honest. I think there are multiple traditions in the U.S. jurisprudential system that I think make it very unlikely that a challenge to that kind of compulsory application or technology installation scheme would raise. So there are two that I'm thinking about. One is frankly a long tradition that dates back more than 100 years that enables the government to enforce quarantines and to enforce vaccination and other of what the government considers to be medically necessary schemes on individuals, and that tradition—the Supreme Court has weighed in on this question in multiple cases.

Mohammad Tajsar: The principle that we can extract from that line of cases is that even though individual liberty is at stake when the government compels you, for instance, to install an app on your phone, that so long as the government claims a larger public health need or benefit to it, that a reviewing court is likely to give the government wide deference in making that determination, such that for instance, if the state of California told us, "Everybody has to install this application on their phone because it's critical to ensuring an orderly reopening of the economy and to ensure that people aren't unnecessarily infected," I think it's going to be difficult to challenge that, and I think the state of California's going to be given wide latitude to make that determination. That doesn't necessarily mean that's a good idea. That's just what I think the Constitution and the laws will authorize as a legal matter than clearly whether it's the right policy or normative thing to do. But I think that's one line of cases that I suspect will likely mean that those challenges that you described, John, are unlikely to be successful.

Mohammad Tajsar: I think the other is we've been living . . . If I were to take this out of the pandemic context and put us in the terrorism context, we've been living for 20 years basically, just short of 20 years, in a global state of emergency brought by the 9/11 attacks and how the U.S. government has responded to those. And if nothing else, what we have learned from how the law has responded to that state of emergency is that, frankly, anything goes when it comes to the government's say-so about what is necessary to respond to

that purported emergency. That is to say that the government is often given, and indeed we've seen this, an extraordinary amount of latitude in making decisions in response to what it unilaterally claims is an exigency or an emergency and that courts will rarely second guess the government in determinations about what's appropriate in response to emergency.

Mohammad Tajsar: I, having worked on these questions for a long time in the ACLU itself as an organization, I've been working on these issues for a long time, is deeply, deeply skeptical of that basic premise that allows the government basically uncontrollable power to conduct whatever it is that it wants to conduct in a state of purported emergency. But I suspect that that history, that precedent, that we have wittingly and unwittingly built over the last 20 years, is likely to give additional fodder for a conclusion that a compulsion in the use of a technically assisted contact tracing program is legitimate. So that's what I would say. I'm skeptical that any such challenge would survive.

John Villasenor: Okay well, here's another question. The government historically has been, shall we say, reticent to part with data that, once acquired, it thinks might be useful. And suppose a government entity were to get detailed location data through some sort of compulsory process or some other process. What are the risks that the government might later decide this information was really useful for things like combating crime and therefore be unwilling to delete it after the pandemic has passed?

Mohammad Tajsar: I think the risk there is tremendous. I mean if there's anything that we have learned from the rise of data-driven policy making, it's that governments have a voracious appetite for data, particularly because the cost to storing information is frankly negligible now. The cost of analyzing information is really high. I mean it takes a lot of time and money to be able to analyze data appropriately, but it's really easy to collect it. And I think what we are seeing, both from the federal government all the way down to local municipalities, is that everybody is eager to collect and eager to figure out what to do with that information on an ad hoc basis, often without real consideration, usually without public input or stakeholder input.

Mohammad Tajsar: And so, that is the context that we find ourselves in today, the context in which the surveillance and data collection ecosystem in this country is extravagant and largely unregulated. And so, we have to really consider whether the use of technology to address this particular pandemic is one that we can countenance in light of a history that is replete with instances of mission creep, instances of abuse of technology, instances where a particular tech that was sold to us to do one thing is instead being sold to us to do another thing.

Mohammad Tajsar: I can give you one quick example, and that's the use of body cameras and facial recognition technology. So body cameras on law enforcement officers were principally sold at the time when they started to become popular as ways to keep officers accountable. If officers had video cameras, you'd be able to see if they engaged in some form of police brutality, for instance, or sexual assault, and that's what the public was told. And the public went along with it in some sense and allocated a bunch of money, and now cops across the country use body cams. But then when they started using body cams, it became increasingly accepted to use body cameras, not as a form of police accountability, but as a tool for criminal investigatory purposes. And that's when we saw cameras being outfitted with a whole bunch of different sophisticated technology, including facial recognition, to actually serve investigatory purposes. So there was a bait and switch when people were told, "No, we're going to use these body cameras to keep officers in check," but instead, they have become surveillance tools. And that's why, for instance in California, a recently passed law prohibited the use of facial recognition on body camera footage precisely because of that bait and switch.

Mohammad Tajsar: Well, you can imagine that also happening in any of these tools or proposals that are being brought to the public's attention with respect to Covid. We really have to be cognizant of how these technologies and how these tools are used and place strict firewalls on them to ensure that they are not exploited in ways that impact people's rights and liberties.

John Villasenor: Thank you. So a related question then is, we talked a moment ago about how the government might sort of attempt to make incidental use of data that they had collected for different purposes. But even if the government doesn't actually have this location data, let's say tracking data, in its custody, if data exists, for example, on the servers of Apple or Google, and if the government knows it's there, won't that inevitably expose that data to downstream seizures for purposes unrelated to combating the pandemic?

Mohammad Tajsar: Oh yeah, absolutely. I mean there is a interconnected web of problems associated with the public and the private industries' access to information about people, and having sensitive information about individuals, whether it's location information if used in a contact tracing proposal or healthcare information, having sensitive information just out there in the ecosystem is likely to result in unauthorized, unaccountable sharing of that information, given that both as a policy and as a technical matter, we do not have proper safeguards over information in this country. So as a technical matter, I think privacy is not [inaudible] into systems by design, and as a result, the systems technically leak a lot of information. They're not designed to store information.

Mohammad Tajsar: And then as a policy matter, we simply have a wild west here when it comes to data and data collection and data aggregation and sharing. There is no federal privacy legislation that can put limitations on, for instance, sharing of data about people by data brokers. There's a unregulated space where private entities can do whatever it is that they want to do, and the public sector can leech onto the work of the private sector in that way. And so, I think we really have to be concerned about how sensitive information about us will be exploited, not merely by the likes of Apple and Google and other technology companies, but how that information can often seep into and be used and exploited by government actors. And that is a real concern that all of us I think should share.

John Villasenor: Thank you. Here's a question just about the global landscape. In many other countries where the civil liberties protections that we have in the United States are absent, governments of course have far fewer constraints on tracking and other forms of data collection. If those countries employ these techniques that, if used here, would be viewed as very significant infringements on civil liberties, and they start to see significant progress against the virus precisely as a result of these sorts of methods, would that create pressures to use those methods here in the United States, and in doing so, create pressures that would tend to undermine civil liberties here?

Mohammad Tajsar: Oh yeah. I think absolutely they would. What we have in this country, as I say, is a extensive, robust, and complicated ecology of surveillance capitalism that is designed to exploit data and make a bunch of money out of it through an interconnected web of small and large companies and small and large government actors. That is to say there's a ton of money in data and surveillance and crime control and all of the like, and that money has created obscene incentives for the use and exploitation of data in this country. So you can imagine if there are either successful or presumed successful applications of technically assisted contact tracing tools, for instance, abroad that the pressure to use them here domestically will be great and immense, and we've seen that already. There's lots of references to systems that are being used and were used in China, South Korea, Israel, and other places really without an adequate nor appropriate understanding, both of how those systems abroad were used, but also of how those systems were implemented in a broader social and public health context that is really not analogous to what we have in the United States.

Mohammad Tajsar: But given the what I think are perverse incentives in the United States to exploit the use of data here, we're unlikely to see the downsides abroad. We're only likely to see what are perceived to be benefits, and the pressures to deploy those technologies are likely to be great. And we've already seen that here, and that are a lot of tools that are being developed and are starting to be rolled out here in the United States without the kind

of thinking and the kind of care that are necessary to ensure that these tools are going to actually be useful. And that I think is a real problem and one that I think we should all be really cognizant about.

John Villasenor: Well, thank you. So I'd like to turn to an issue which involves the intersection of medical privacy and digital privacy, and there's been quite a lot of discussion recently about doing widespread antibody testing and giving people who have antibodies for Covif-19 what's sometimes been called an "immunity passport" that gives them more freedom to work and travel. Let's put aside for the moment the question of whether in fact having antibodies actually confers immunity or not, assuming for the moment that it does, and it may not of course. But if it does, that implies that people who don't have antibodies would be disfavored under the law in terms of their right to work and travel, and do you worry that this approach would create a new formally disfavored underclass of people? And what are the civil liberties concerns that we would see?

Mohammad Tajsar: Yeah, I mean absolutely I do, and the reason why I do is I think less a technology-based reason, but more a political and economic reason. That is to say that what we have seen just in the short amount of time that this disease has raged in at least the United States is that all of the traditional structural barriers to healthcare that exist in the United States have exacerbated the disease's impacts on communities across the country. So that is to say you are more likely to survive this disease if you are rich, if you are white, if you have access to medical care. That's a fact.

Mohammad Tajsar: So what does that mean if there's a widespread adoption of the kind of immunity passport protocols or the kinds of things that you're describing, John? What does it mean for those reopening proposals to be adopted in the country in which there is a stark differential access to the kinds of tools that will make antibodies available on a just and equitable basis? What it means is that the people who are likely to get the kind of immunities that are necessary for them to go back to work are people who have access to the kind of treatment that allows them to get the antibodies, and those people are going to be people that have the kind of means, the access, the social and political power to be able to give them the healthcare that they need.

Mohammad Tajsar: And what will inevitably result is a massive underclass of people who don't have those means, who don't have that access, who don't have the ability to take care of themselves and their families and who are locked out from portions of the economy that they need to survive, and it's kind of perverse because at the same time that that might end up being what occurs, what we have seen is that those people in some places are actually being forced to go back to work on the threat of losing their jobs in these states that are opening, in my view, prematurely. And so, at the same time

that there is a complete lack of disregard for their safety, proposals that will reopen the economy based on immunities are likely also to exclude these people. So either circumstance, the massive underclass of people who lack political, economic, and healthcare, who lack access to the levers of political and social power are going to be screwed either way, and I think that is really a symptom of just persistent latent inequalities in the United States.

John Villasenor: And to expand on that, it seems that if there was such an immunity passport, you might imagine that that could create incentives for people who don't have the financial resources to just simply hunker down to actually intentionally go out and just get infected so they can get the passport because that's what allows them to work. And of course if they did that, they would also be placing themselves and their families at risk.

Mohammad Tajsar: Yeah, absolutely.

John Villasenor: I think the inequities are amplified in that context, right?

Mohammad Tajsar: I think that that's absolutely right, and that's just the kind of social and political context that the immunity passport proposal finds itself in. Then we have to deal with the actual design of those systems itself, which I'm deeply skeptical of because those systems require a whole host of information and data about people and that require a real thought in terms of how they're deployed. So just to give you an example, in order for me to get an immunity passport, let's say it's an application, I have to upload my own data to that system. That system then needs to verify that I am who I say I am, that I indeed have the antibodies myself. Who knows how that will happen? And then it needs to make sure that when I do go out, that somehow I'm not just giving my phone to somebody else for them to use, and then that system also has to preserve all that information that it has, somehow interact with other places, like for instance a movie theater or a live sporting event.

Mohammad Tajsar: There has to be some kind of facilitated exchange of information, and it's not at all clear how to maintain autonomy and privacy in that context and prevent the kinds of potential abuses that we were talking about in this conversation. So I think there are a lot of technical problems associated with that proposal even after we resolve the latent social and political problems, which I don't think we're going to solve.

John Villasenor: Right, and that leads to my last question here, and you already brought this up quite rightly. There's a lot of evidence that the suffering and the economic harms, the health challenges caused by Covid-19, those things are falling disproportionately on communities of color, communities with fewer economic resources, and when we talk about these sorts of potential

civil liberties infringements, digital privacy infringements, other concerns arising from the pandemic, is there a concern that those would fall disproportionately on those same communities? And how can those concerns be addressed?

Mohammad Tajsar: Oh absolutely. I mean I think that there is I'd say two things, two facts, two assumptions that we have to make here. One is we have to assume that access to technological tools to solve people's lives or to make things easier is an access that is mediated by power. That is an assumption that we have to assume is true because the history of technology demonstrates that that is in fact true. So if you have a immunity passport system that's based on phones, then what that means is people who don't have phones are locked out. People who have good access to internet, for instance, are the ones who would be preferred in a system like that versus people who don't.

Mohammad Tajsar: Remote learning, for instance, is creating a situation in which students who come from wealthier backgrounds are more likely to be engaged in school, whereas those who don't, who have maybe child care or sibling care or family responsibilities, are being shut out of the remote learning environment. So everything that we know about technology today suggests that there are differential impacts on the widespread adoption of a whole host of different technological tools in our society. So that's the first part.

Mohammad Tajsar: And then if you couple that with the data that is coming out as a result of Covid that shows in plain and stark terms precisely what you're talking about, John, that the disease is impacting people of color and poorer people at astonishing rates as compared to their whiter and more wealthier peers, what you have is a recipe for disaster, I think. So just in, for instance, reporting earlier this month said that the rate that blacks in Chicago are dying as a result of Covid-19 is at just about 6% higher than the rates of white people. Here in L.A. County for instance, there have been something like 940 deaths or so. We have data around 860 of them, and of that 860, 14% are African-Americans. But the African-Americans make up only 9% of the county's residents. So they're dying at a disproportionately higher rate, and that's true across the board across the country.

Mohammad Tajsar: So all of that to say we have a unique problem when it comes to particular communities like people of color, like the elderly, like people who are incarcerated, are uniquely exposed to the risk of coronavirus, and so long as these technologies do not attend to those communities, we are unlikely to be in a place where we resolve this pandemic for the good of all of us. If these technologies don't, for instance, address the principle epicenters of the epidemic today, which are nursing homes and jails, then we're not

going to be in a place where we can fully reopen this country and bring some real normalcy back because the virus will continue to live amongst our elderly, amongst the people that we detain in immigration prisons, amongst the people that we detain in jails across the country.

Mohammad Tajsar: So whatever the technical solutions are, whatever the technological tools are that we develop, they have to be uniquely tuned to the least among us because it is the least among us who enable us to get back to the kind of normalcy that we all are craving right now, and I think that's going to be really important.

John: Villasenor Thank you very much. I guess I'll just ask if there's any closing thoughts that you'd have to offer before we wrap things up.

Mohammad Tajsar: Yeah, we've had a conversation about technology, and I guess what I want to do is end with one tool, one sort of reminder, that I think should give us some hope. And that is given all of the problems associated with technology, there is in fact a way for us to do all of these things, to address all of these problems, in a way that actually has a light at the end of the tunnel, and that tool is human-to-human contact. That is the kind of humanity associated with the care for each other, both inside the medical system but also elsewhere. That kind of contact is actually the kind that is more likely to be effective in addressing this pandemic than any of the technological tools that we are thinking about or devising.

Mohammad Tajsar: So all of that to say there is a real important place for manual contact tracing, contact tracing that's based upon interviews with human beings that bring comfort to those who are affected. It is one thing for me to receive a text that I may have been impacted, but it's quite another thing for an actual human being to call me and talk to me about why that is a potential problem. And this is not just me saying this. This is epidemiologists across the spectrum are saying that there really is no substitute for human contact, for the types of tools that have helped us get out of epidemics in the past and that these things are potentially only real sideshows to the real solution that'll get us out of this. And those real solutions are solutions based on people and of love and compassion, and I think I would like to leave us with a reminder that it is only us that can bring each other out of this abyss. And it's not the tools that we hide behind, and I hope that that comes across in the way that we think about this going forward.

John Villasenor: Well, I thank you very much. I'm very, very much appreciative of your willingness to spend some time answering these questions, and thank you again for your time.

Mohammad Tajsar: I appreciate it, John. Thank you so much for this opportunity.