Transcript generated by Temi.

DANIEL CASTRO:

(00:00)
Hello and welcome to today's ITIF webinar. My name is Daniel Castro, and I'm vice president of the Information Technology and Innovation Foundation. The topic we're exploring today is how much privacy should we trade to survive a pandemic. I'm joined today by AL GIDARI, director of privacy at the Center for Internet and Society at Stanford Law School; RACHEL LEVINSON-WALDMAN, senior counsel in the Liberty and National Security program at the Brennan Center for Justice at NYU School of Law; and PETER MICEK, general counsel at Access Now, an advocacy group focused on digital riots.

(00:37)
So, welcome everyone. For those of you that are joining us in the online stream, you're welcome to ask questions to the panelist at any time during the event. If you're watching on itif.org, you can use the Q&A form under the video. And if you're watching this video directly on YouTube, you can follow the link in the event description, to get to the Q&A form.

(01:04)
So to begin the discussion, I want to highlight at least two scenarios that we see right now for how personal data might be used to track or monitor individuals during a pandemic. So the first one that we're hearing about is really around analyzing broad trends. So for example, you know, looking at an analysis of aggregate data and how that might provide insight into the level of adherence to physical distancing in different communities or using that data to predict future hotspots by looking at different types of regional population flows.

(01:37)
And the second scenario is looking at more granular personal information. And so here the question is, can we trace specific movements of individuals to identify where they went and whom they might've come into contact with? We've seen a lot of research recently come out arguing that very fast contact tracing to the level of instant notification when somebody receives a diagnosis, alerting their contacts that, you know, you might have come into contact with this person that can make a difference in flattening the curve. Rachel, maybe I can go with you first. My question is, you know, should the U.S. government and the U.S. government public health officials or researchers working in this space be using more of this type of personal data, and if so, what types of data should they be looking at?

RACHEL LEVINSON-WALDMAN:

(02:25)
Sure. Thanks for the question and thanks for having me on this.

(02:28)
I think that we might answer that question differently at different times, right? And just, sort of, you know, coronavirus vs. non-coronavirus sort of different stages of the spread of coronavirus in the United States and the response to it. So I'm not a public health expert. Based on sort of what I've been reading so far, it seems that in the earlier stages of the epidemic here that that kind of individualized contract tracing had a real role to play. And certainly when you're talking about diseases that in some ways are actually less transmissible and require closer contact. So, for instance, some public health authorities have drawn a distinction between coronavirus and something like SARS or MERS that had way fewer cases and also were harder to transmit and required people to be in contact. So it's really incredibly useful to know if you've been near somebody who's infected. You can take the appropriate steps. And there is sort of a limited number of cases you could do that labor-intensive contract tracing with. It looks like at this point, given the spread of coronavirus in the United States, that in a lot of ways contact tracing just isn't the most efficacious thing right now. And here I am talking I guess about individualized contact tracing, right? The kind of, you know, you go to your home and find out that you're infected, who you've been in contact with? And contact them. Or I find out that somebody that you've been near has been infected. I'm going to reach out specifically to you. When we have both the kind of rod, we just know that there are tens of thousands, I think at this point, hundreds of thousands reported cases in the United States. And wide transmission and a lot of asymptomatic transmission that it's not as useful. But on the other side, right once we actually have flattened the curve, when there are way, way, way fewer cases, it may go back to being fairly effective, still labor-intensive, but an effective method to use. Which I do think can be distinguished from using aggregated data to look at things like our general population movements, to what extent are social distancing requirements making sense, how far people are moving from their home, are they traveling down particular roads or bridges, which I could see being a very useful tool for policymakers and for public health officials.

DANIEL CASTRO:

(05:00)
Great. Thanks, Rachel. Al, do you want to weigh in on this as well?

AL GIDARI:

(05:05)
Yeah, so I have a different perspective than Rachel on this. And a lot of it stems from the public health authorities, the local level who are overwhelmed with contact tracing. Contract tracing has value throughout the entire life cycle of a pandemic. It is the only thing that prevents a complete shutdown in general lockdown and an overbroad way of dealing with the pandemic. So contact tracing allows you to be more surgical and more pointed. It has valued from the start in order to identify common areas where individuals have been. Because contact tracing is not just about the individual, it's also about the place and the time. So when you can learn that 30 people were in the same place three days ago and they all have it, that tells you a lot about that place and, giving other people who were there at the time and place, early warning to self-isolate. It is one of the most effective ways to communicate the trajectory of that disease in a community. Because what happens now is that the public health authorities are understaffed. It's the most frustrating job in the world for them to try to reach people. And the individuals already are sharing all of the data with the government. So this isn't a case of compelled disclosure by the government. It's a case of how do we make the contact tracing the transmission of information more efficient so you can deliver it to the marketplace quicker. Pulling from an individual's CDRs, the call detail records for location information, as far back as 2010 case studies by epidemiologists have shown to be a really effective way to help. And it's an augmentation for the information the individual provides; it's not a substitute, but it makes it incredibly more efficient to be able to understand where someone has been particularly in an asymptomatic disease environment like this where you don't know if you have it or who was carrying it at the time. So that methodology can be streamlined and deployed immediately. And that really relieves the anxiety in the community because nobody knows when your county just tells you there are three cases in your county. Well, where? Which town? Which place did they all get it from? I mean, those are really helpful things to know at the ground level. And right now the system is really broken. It is totally localized and randomized. And as a result, it just doesn't work very well where we could really improve. And, last point is, Rachel said, it is true that as it ebbs and flows, it becomes more important. When we come out of this general lockdown, we're going to have a resurgence and that contact tracing is going to be all the more important in the second go-around if you will, or the third go-around. So getting the system right at the front end, is really important and we just haven't done very well with that right now for a variety of reasons.

DANIEL CASTRO:

(08:32)
Thanks, Al. Peter, I want bring you on this as well. You've written recently about this issue. I thought it was interesting in the new report you have out that you note that, you know, these are unusual times that, you know, this is not the normal situation. And that even though a lot of people talk about privacy being a fundamental human right in these times of crisis, you still make adjustments. And, you know, I wanted to get your perspective on, you know, what should the government be doing now and how it's balancing against these fundamental rights that, some governments encode or (inaudible).

PETER MICEK:

(09:10)
Thank you. Yes, human rights law still applies and international law still applies even in times of crisis. That's a point that we want to make clear that this isn't an extra-legal scenario, that actually we operate under frameworks that envision that at times emergencies arise, disasters and crises occur. And there are provisions in international legal instruments that the U.S. and every other country has signed on to that allow for temporary derogation that, you know, set out the processes that governments should take to announce and to specify and time-limit these extraordinary circumstances. The right to privacy, the fundamental right to data protection, and the right to freedom of expression still do apply. They aren't absolute. In a lot of national laws and in international instruments, public health is a specified reason to at times interfere with the exercise of these rights. However, any interference needs to be strictly necessary and proportionate and there has to be a purpose. That's clear. So you know, when we're talking about call detail records, those include information. I can include location data on impacting our right to travel. Their sharing infringes on the right to privacy because the metadata shows we were talking with where we're going, along with (inaudible), etc.. So there is an interference there, and we're very concerned that there'll be a rush to not just collect it all but share it all. And we've seen from previous crises, like the Ebola response, that call detail records aren't necessarily going to make the government's response more efficient or targeted. But meanwhile, their sharing will end up impacting the right to privacy, and perhaps creating longterm trust issues and gaps where people don't really feel like they want to consent to what even well-meaning and well-intentioned efforts in disaster response because they've seen how their data is used again and again, after these crises occur. I'm happy to say that our paper came out on recommendations to governments on how to protect data, how to uphold data protection principles while still engaging vigorously in this fight. It is out on our website at accessnow.org. And we say that two overruling messages: first, protecting digital rights can promote public health, and second, that the question is not whether or if, but actually how

government authorities should use health data in crafting a more efficient rights-respecting response.

DANIEL CASTRO:

(12:24)
Thanks, Peter. Why don't we stick on that question for a moment, and I can start with you, Peter. We can then go around. To that question about what type of data should be used, how do we actually do this? I think that one of the core questions in what data should we be using? Is it, is it health data? Is it more this location, location data coming from different sources? You know, we've seen some countries looking at payment data. So there's a lot of different potential data sources on the table. How should we be thinking about which data the government should have access to and which present more risk or less risk? Have you gotten into that in some of your work now, and why don't we start with that?

PETER MICEK:

(13:04)
Yeah, thank you. So our paper does focus on those two main areas, types of data that are being requested, demanded, and shared. The first thing, tracking location and geolocation data, and the second thing is health data, however broadly that is defined. So those seem to be what's at issue. We also speak to public-private partnerships, which of course, span the range from apps to data storage to (telco) transmission networks. So, those are the two main areas. What we would say is that I think public health experts should be the ones leading this discussion. We are very concerned that governments are apt to find any excuse they can to get their foot into the door of the massive stores of data that the private sector holds, and use that data for all sorts of law enforcement purposes or you name it. So surveillance is a bad party guest that stays much longer than you welcome it for. So we would want to be sure that there is civilian oversight, specifically from the health community, in determining what data is going to be efficient for the purpose of fighting this pandemic, and that there are written agreements with some set clauses and rights-respecting ways that limit the use, the retention and the data-sharing agreements in time and in scope.

DANIEL CASTRO:

(14:51)
Thanks. Rachel, can you expand on that too? I'd be curious about your kind of impression of the direction we're going right now. Having your experience in national security, you've seen this debate, of course, play out many times. Whenever there's an incident people say we need

more information. Do you think we're in that same type of scenario right now? Or do you think that this is a little bit different in the sense that this is, you know, maybe a little more unprecedented? We haven't had this kind of global health situation. It's not the same where perhaps with national security we consistently see national security saying, we want more data, we want more data, we want more data; on the health side, they're not the ones that are typically in these forums saying, we want more data. So I guess my question is, you know, I totally understand what Peter is saying, but I'm also wondering, you know, to what extent is public health maybe different than the typical national security debate?

RACHEL LEVINSON-WALDMAN:

(15:51)
Yeah, I mean I think in some ways my answer is all of the above. And I would really plus one a lot of what Peter said and I would really command of the AccessNow report for folks who haven't seen it. It's really helpful and really interesting. It goes through the data well and it has really thought-provoking case studies as well, which I think are really a nice entrance point to thinking about these issues. So I guess a few thoughts -- and let me see if I can sort of remember all the things that came up for me as you were posing your question, Daniel. So I guess, you know, I think one of the main things that you were asking is are there sort of lessons learned from the national security context and to what extent are we in a different realm here? And I do think the answer is sort of 'Yes' to both. On the one hand, sort of to the point that you were making at the end, I think it's important who's going to be using the information. Right? So I think there's always a concern in a national security context that when there's a push for more information, it is going straight into, you know, some combination of intelligence community and law enforcement. And so the stakes are very high, right? So when you're talking about agencies getting this information in that have the power to prosecute, the power to surveil, the power to detain and deport, you want there to be a high bar or how it's collecting information, for how much information they're collecting, what they're doing with it, although I think those backend restrictions are just as important if not more so here. But there are real concerns about even kind of the initial intake of the information and it's often and not necessarily to kind of suppose bad faith, but it's kind of the people who are arguing for the intake of this information that often then do want to use it for other purposes down the line. Right? You might see a value for sort of the mission creep or surveillance group. Those considerations are different, at least somewhat different when we're talking about the public health context, right? If it's public health officials that are saying that there are kinds of information that would be useful for this purpose, I would take that very, very seriously. I think there is enormous value. I think it's critical to have public health expertise be really front and center in this discussion in terms of what kinds of data are going to be useful for public health interventions, how should it be used. Even questions around who should have access to it. I

think that's really, really important. By the same token, I do think there are still sort of broadly lessons learned about what we do in times of crisis, right? And how we respond. We know that kind of post 9/11 and that time of crisis. There were a lot of programs rolled out kind of under the justification of we need these to fight terrorism, right? We're under this existential threat and we need to collect more information. We need to put it all in one place. We need to have these sharing processes in place because that's the only way that we're going to kind of prevent the next terrorist attack. And then you can look back, you know, sometimes years down the line sometimes, you know, kind of at the moment and say, hey, some of these programs, massive, massive data collection. Afterward there were national security officials or Homeland security officials who said, actually we brought in more than we could even use that didn't turn out to be useful. Programs like NSEERS, which was interviews with and registration of individuals of men from Arab countries. Which was sort of obviously discriminatory on its face. Also didn't actually produce any prosecutions. I think sort of broadening out, I think those are notes of caution to think about when we are in times of crisis and we do need to sort of step back and think about (whether) we're getting in the right kinds of expertise. Is this data that's actually going to be useful and how? And then I think especially to Peter's point, thinking really carefully now, not later, but now, about how's this data going to be used, who is it going to be shared with? If it's in the hands of public health officials under what circumstances, if any, does it get handed over to law enforcement? How long is it kept for? There might be research purposes for which it's really useful to have some of this information down the line. But on a very granular level, what do the restrictions look like around how it's kept, in whose hands or how long, who it's shared with, kind of all of those things.

DANIEL CASTRO:

(20:32)
Thank you. And so, Al, feel free to react to anything you heard, but I also wanted to ask you: one of the questions I think keeps coming up in a lot of people's minds is this question of we would be supportive of this if we know it's effective. But to know if it's effective, we know in theory it's effective, we've seen lots of models saying that instant notification would be useful, but the question is in practice, can this actually be achieved? The problem is you can't actually know in practice if it can be achieved unless you try it out. So it's a little bit of a chicken and egg dynamic here. And so I think one of the questions that's on the table is to what extent can right now government officials, companies that have this data, start using it for public health purposes to see if it works in a pilot or trial phase just like we're trialing other things. Does the current law or laws currently allow this type of flexibility so that location data and other types of data can actually be used in an experimental public health purpose?

AL GIDARI:

(21:38)
There's a lot in that question. The legal framework really doesn't contemplate pandemics. And so you have the Stored Communications Act and that limits what providers and platforms can do with individual data. And without a person's consent or a voluntary disclosure in the case of an emergency, a company can't use that information. We have both. And with contact tracing, we have individualized consent. And I think it's pretty clear we're in an emergency situation. So the providers, the platforms, are in a unique position to say yes or no over what type of data gets used and for what purpose. And I think legally they can cooperate with government agencies to do tests and experimentation on that. And that provision in the law includes both individually identifiable and aggregate data. So, like it or not, it's a system we've lived under for 40 years with the Stored Communications Act and something that happens all the time when a kidnapping of a child at a state fair occurs, (telcos) dump the tower that's carrying all the cell phone signals in the area to see if they can figure out who might have abducted the child. That's an emergency disclosure. This has been going for a long time. What I think is true is that we've never had a system on the back-end to limit what the government does to it. And you know, Peter's comments are exactly right here. You never need to know what those safeguards are until you don't have them. And here even the title of this program, do we need to give up privacy for fighting the pandemic, is almost the backward question. It's whether you need to give up privacy to fight the pandemic so I can stay healthy. It's your privacy. We're talking about not mine, I'm healthy, and so I'm not worried about it, but I want to know who has it. And that really becomes the mentality in the community and it becomes the mentality in government. And so those safeguards are missing. They've been missing for 40 years. They ought to be put into place, but when you don't have the urgency or the need, there are other priorities that really get the attention. And certainly since 9/11 we've had a lot of other priorities and haven't thought about pandemics. I'd also like to just comment on the notion that the epidemiology and public health community should be determining the answers here. Critical to have them. And it's critical also that over the last decade they have used location information in the aggregate to good effect to determine a trajectory in density of the disease. Those studies are out there and we shouldn't ignore those. It's also true that public health is overwhelmed by data. And so more data isn't always the answer either, but more efficient use of that data, like in contact-tracing, which is a heavily manual process, could really help them. And so that's the pragmatic answer there. But I also think that the public health community, at least in the last three weeks of discussions I've had with some really smart people that do this for a living, they don't know all the capabilities that are out there or all the data sources that might work. So having a collaboration between the smart lawyers that I see on Twitter all the time with comments and the smart epidemiologists will only improve it, but then Peter needs to be there so he can make sure the framework for protecting the personal information is in place. So there

really is a three-party discussion that we ought to take away from this going forward because we are going to need this again and we will need it more, as we get through this process and come out of lockdown and we have a resurgence.

DANIEL CASTRO:

(26:09)
Great. Thank you. Peter, I want to turn back to you, picking up on Al's point about the legal framework does not contemplate pandemics, I wanted to ask you to react to that in particular. You know, one of the things that struck me recently was that Santa Clara County came out with some statements saying that they weren't able to disclose some public information about, which cities within their county had infections because of the fact that they didn't think federal privacy allowed them to do that. And we've seen in the EU, some member states like Italy create these temporary carve-outs for data collection and sharing, that are time-limited, that are focused on the outbreak specifically. And I guess my question for you is is that the right approach? Do we need just some temporary carve-outs? Do organizations have sufficient flexibility or is it just kind of misinformation about what the law allows and you're seeing maybe some information sharing not occurring when it could actually occur legally?

PETER MICEK:

(27:17)
Thanks. So first of all, I do trust a lot (inaudible) on privacy issues. Generally, it's been a leading, actually, kind of putting in place civilian oversight rules on procurement of surveillance type, for example. Not in (inaudible) issue right now as a lot of the bigger surveillance tech purveyors are selling their snake oil to governments right now as a solution in this fight. Setting that aside, it's a very valid question. One thing we're pushing for is to get agreements in writing. Right now what we think is happening is essentially phone calls between, for example, European telcos and governments. There's been reporting on the role of the GSMA and others in arranging this supposedly global sort of reaching surveillance system for response. We want to see in writing, you know, what's, taking place, what's being agreed to and the legal basis again, for this. And there should be a legal basis again to respond in law. I don't actually focus on the U.S., but I understand there are emergency provisions. Maybe pandemic wasn't what was thought of. I know the focus has been on terrorism, but there should be in most data protection laws, certainly, rules that can be laid out on paper. We want to see these agreements written out with some set clauses, oversight provisions, and secondly, that civil society should be brought into these discussions. So thank you, that's a great point that this should be a multi-party discussion taking place led by public health officials, but that civil society is a key partner. And finally, on protecting individuals, we do see, you know, great threats to individuals who've been

identified by public health authorities inadvertently or not. There have been cases of death threats against people who are suspected or reported to be infected in the last few weeks. And throwing this onto the fire of the existing inequalities in the world and things already put people at risk, like being an ethnic minority or from low-income community. as we see this spread globally, I fully fear that public messaging from authorities on who is and isn't infected, is going to be weaponized itself. And so it's another reason that we see the need and I do believe there are ways. Contact tracing presumably involves consent. People probably wouldn't consent to that. Ways that people can be, civic-protected, but also give enough information to enable an efficient response.

DANIEL CASTRO:

(30:23)
Thanks for that, Peter. I hear you saying, and I think other people have said this as well, you know, this idea that if we move forward in this space, we need to have, you know, very clearly defined rules. I guess my question for you, Rachel, is, do you think that's something this administration is doing or should do when, you know, for example, CMS today announced the basically, you know, they're ripping up the regulations for a whole host of areas from oversight of in-person visits to nursing homes. They're dropping the paperwork requirements for physicians. They're basically saying, you know, all this red tape, it needs to go temporarily. We just need to focus on solutions. And so I guess my question is, you know, maybe it's two-folded. Obviously in an ideal scenario, you would keep regulations in place. They're usually there for a reason or if they're there for a reason, they shouldn't be maintained. I guess the question is do you think privacy should be an exception here, to kind of where regulation, being kind of stripped away, is occurring, and do you think that's likely to occur in this administration?

RACHEL LEVINSON-WALDMAN:

(31:38)
Right. It sounds like there's a few different questions, but I think the question is, is this administration likely to pay close attention to concerns about privacy and downstream use? No, probably not. I mean, I think one of the big concerns, and I think Peter touched on this as well, has been, how would this data be used down the line? And not just in sort of a hypothetical way, but given everything we know about this administration's war on immigrant communities, so various ways you could see data being used for increased detentions and deportations, and you know, is it going to be used down the line for other kinds of surveillance for targeting? I do not put sort of high hopes in this administration for imposing, tight restrictions. That being said, I suppose there are a few thoughts. One is, to the extent that a lot of this is through the states, right? So they're saying that states are sort of controlling the collection and some dissemination

of data. Then there could be much more state control. I mean I think there's still sort of concern in terms of how granular the data... So for instance, if there's granular location data that's being shared from various kinds of companies, right? There are going to be limitations in terms of, for instance, what telecoms can do, sort of what information sharing looks like, you know, straight from a telecom provider. But I think those restrictions sort of ease up as you get to say app developers, data brokers, right? There's a lot more ability to sort of just share the information that's been collected. So certainly in terms of that information going straight to the federal government, I think there are a lot of concerns about how it would be used if it's either, you know, individualized now or could be individualized down the line. You know, conceivably that's an argument for really calling on the corporate sector to kind of tie its hands to some extent in terms of what it's sharing and how, to, you know, take some responsibility for how it can be used. But then again, I guess going back to thinking about public health data, to the extent that that's being collected and used at the state level, then maybe there's more reason to be optimistic, at least in some areas for sort of restrictions that would be put on that data. And I guess more generally, I think one of your questions was, if I was hearing it right, sort of, is this the time to be worried about privacy, right? You had made a reference to should privacy be an exception, right? Is this a time that we should be focusing on privacy concerns? And I think it absolutely is. I think it's absolutely reasonable to think in different circumstances about how we balance the value of privacy as against other societal values. There is a strong societal value of being able to leave your house and go to a paying job and interact with people and not come down with a potentially fatal disease. At various times we think about how to (keep) these various considerations into account and how to weight them. But I don't think that there's a scenario in which we say, or in which I would want to say, well privacy just gets shunted aside. Because that will have so many downstream consequences and I don't think that is what we need to effectively fight coronavirus, to say, you know, for awhile we're just not thinking about privacy at all.

DANIEL CASTRO:

(35:34)
Thanks. So Al, wanted to turn to one last question. We have a lot of questions coming in from the audience and I want to turn to those. The last question I had for you before we do that is around this question of whether companies can turn over PII to the government. We see a lot of privacy policies so we're talking about commercial data, not physician data. We see a lot of companies say in their privacy policies that, unless required by law, they won't turn over this information to the government. So when you have a kidnapping in the scenario you raised before, there's a clear legal compulsion to turn over that information there can be. As you noted earlier, a lot of people never really contemplated this idea of a pandemic. So the

question is can businesses unilaterally decide to share consumer data for public health purposes? Do they have that ability right now under their own privacy terms?

AL GIDARI:

(36:30)
I think that actually, the provision that you find in every privacy policy says exactly what you say and then goes on to say, except in an emergency situation where the life of someone may be immediately threatened. So the emergency exception in the Stored Communications Act and in Section 222 of Title 47 in the Communications Act both permit the nonconsensual disclosure of personal information and communications content to the government if there is an emergency that involves serious injury or the death of another. And you'll find that in every privacy policy. So like it or not, it is the world we've lived in for a very long time. It's just that we haven't thought about it on the scale where we're talking about the disclosure of hundreds of thousands of data points of hundreds of thousands of individuals. And so the providers in this situation really have an important role to play to exercise restraint, to think through whether or not the disclosure makes sense in that case because the disclosure is voluntary. In an emergency situation, government has absolutely no way under existing law, in the Stored Communications Act to compel Google or Facebook or anyone else to disclose location information to fight a pandemic. This isn't one of the exceptions. If it were a criminal case, they could do that, but otherwise, they don't have the ability to compel it. They would need new legislation to do that. And unfortunately, some states are actually talking about new legislation to do that, to require you to download an app that will report your location if you've been identified as someone who needs to isolate or be quarantined. If we get to that world, we're going to have some serious privacy issues to discuss. But right now the collaboration that's ongoing is based on an emergency exception and based on the voluntary disclosure by providers and we are in a position of having to trust them. I will add though, one comment Peter made a minute ago about snake oil because there are a lot of third-party apps, which if the provenance of the consent that they receive from you to use their app, did anything but explain how the location information would be collected or used. So in those cases, we should absolutely reject those third-party apps who are selling the location data. We don't trust the security. We don't trust the source of it and its completeness. And, at least with the big providers, many of whom are under consent decrees, you can hold them accountable much more easily than you can trace one of these mysterious third-party app providers who've been sucking the location out of your phone forever without you really knowing it. So if we're going to have this system where the emergency exception applies and data is going to be shared, I like it a lot better when I know who the provider is and I know that there's an agency that can take the appropriate steps if it's misused. I wish there was a better system for knowing which agencies in the government after the data was provided had access to it and used it, but that's

a really good academic exercise for the future because I doubt we would ever get legislation passed to accomplish that right now. So we are in the here and now and the pragmatic answer of trusting the systems we have in place and the providers that, while we may not be happy with, we can trust more than others is probably the best we can have at this point.

DANIEL CASTRO:

(40:48)
Thank you for that. I want to flag for everyone watching that. If you're watching on ITIF.org, you can use the Q&A form under the video to ask questions. If you're watching on YouTube, you can follow the link in the event description to ask questions. We're going to turn to those questions right now and I wanted to let you know, you can also vote on the questions. So if there's a question you're most interested in, please vote on that and we'll try and get to the most popular ones first. The first question I have, starting with you, Rachel, is what are the risks that need to be managed when collecting and sharing data and how can we manage these risks, especially for marginalized communities?

RACHEL LEVINSON-WALDMAN:

(41:29)
I think the question about marginalized communities is a really interesting one. In the work that we do at the Brennan Center, one of the things that we're thinking about a lot is in terms of surveillance technologies and the national security context and the (policy) context, what's the disparate impact? There's usually a disparate impact. What is the disparate impact of those technologies going to be on marginalized communities? So often meaning communities of color, religious minorities, especially in Muslim communities in this country, and immigrant communities; I think (those stand) out, but also other marginalized communities, LGBTQ communities and things like that. And that's been one of the things I think we've been thinking through in this context, right? As we're talking about sort of all of these surveillance tools being rolled out, maybe being rolled out and tested out, how is that likely to affect marginalized communities in particular? You think, on the one hand, you know, unfortunately, coronavirus is likely to effect certainly poor communities, especially for a combination of kind of density of living, at least if you're talking about densely populated poor communities, right? The closer people are to each other, we know the more likely they are to transmit the disease, and also lower access to healthcare, kind of barriers to healthcare. Obviously that's especially an issue for immigrant communities more generally communities of color and poor communities and also starting just at a lower baseline in terms of health. So communities of color especially are starting at a lower baseline. So then even if they are accessing healthcare, they might have poor outcomes anyway. So on the one hand, you know, if there are interventions that work, I think

it's incredibly important to see those focused in addition on marginalized communities, right? And sort of thinking about how those can sort of help mitigate the effect of the pandemic for everyone. On the flip side though, I think there are a few sort of factors to keep in mind. So one is the extent to which there's going to be less tech saturation in poor neighborhoods and in communities of color. So for instance, phones. We know that at this point, in this country, there are more phones than there are people, but that is still likely to be sort of at a lower level, in more marginalized communities, in terms of, you know, how many phones, does every member of a household have a phone or some other kind of device. If you're talking about using other kinds of location information, you know, to what extent are those tools actually sort of in use by or accessible by (inaudible) these communities. I think another big issue is enforcement, right? So at this point, certainly I'm in Washington, D.C. We are under a stay-at-home order. I think at this point New York is under a stay-at-home order, right? They're sort of spreading across the United States as, to a large extent, they should, and they're becoming more and more restrictive. It has just become more restrictive in D.C. as of today. I am fortunately in a very good position to follow that stay-at-home order because I live in a single-family house. I can work from home. I don't have to go and get on public transportation to get to my job. But obviously that's not true for many people in marginalized communities. And to the extent that these orders are going to be actually policed by law enforcement then folks who have less of an ability to comply with the orders are more likely to be affected by that policing, and obviously there's a big discussion right now also about how this is playing out in jails and detention facilities where people are especially going to be at higher risk. And then again, I think this is where these questions come up about how is this data used down the line for surveillance, for detention for, you know, marginalization including even public health data. You can look back to the AIDS crisis, discussions around use of identifiable information, and how that was actually used to kind of shame and marginalized people more, and then. And then just to Al's point earlier thinking about how apps that are collecting this data or that, are we going to see some kinds of digital redlining, you know. So if you have certain health outcomes or you were determined to be infected at certain times, how is that going to potentially affect your ability to then go back and take part in society in ways that are separate from the actual public health considerations? If you were infected a week ago, there are ways that you should be very significantly limited, right? You shouldn't be out interacting with people but more down the line and how that's (inaudible). So that was a long answer but I think that's a really important piece to have as part of the discussion, being sure that services and interventions are equally available but not in ways that are going to sort of more ill-serve marginalized communities.

DANIEL CASTRO:

(46:09)
So the next question, and Peter, maybe you can take this one, someone asked: EU data protection regulators seem to have acted more quickly to decide that the authorities could use mobile location data. Why did it take longer in the U.S.?

PETER MICEK:

(46:25)
Right. Well, there's a lot of factors into that, including just the seriousness with which the regulars take the pandemic and when it struck. I think it's important to note that this widespread sense that, you know, Europeans care more about data than Americans, about data privacy than Americans do, it's much more nuanced. We've seen really in tandem with the rollout of the General Data Protection Regulation in the EU and those protections, a continue to push by law enforcement and intelligence across the EU for greater access to data for their purposes. So it's not such a clear picture. Europeans also are quite skeptical of how their governments use data. It does seem like there's been more reporting by European regulators making outreach to the telcos. I would say yes, there is quite a history of government backing of certain telcos there, a lot of government interest in some of the major telcos that operate across Europe. Maybe they have quicker channels of communication. They've already engaged in deep discussions around E-privacy Act, around (passing) name records, and other things. So these are active discussions there and there might just be less friction.

DANIEL CASTRO:

(48:07)
Thank you. AI, I am going to go to you for this next question. Someone asked Congress continues to work on consumer data privacy bills using the phrase "precise geolocation data". What lessons has the pandemic provided for this topic?

AL GIDARI:

(48:23)
That's a great question because, amongst many technologists, you have incredibly different opinions on how precise geolocation data is. It has been interesting to me in this discussion generally over the last month that a lot of privacy advocates have argued that geolocation isn't precise enough to be helpful here. At the same time, privacy advocates who are screaming that it's so sensitive, how can we use it? We let anybody use it or have it. So there's a little

incongruity here. The fact is that it is extremely precise. It can be extremely precise depending on the application it comes from. Not all location is created equal. Location from WiFi is different from GPS, is different from what you get in Google Maps. I think, if there's any lesson to be learned out of it, particularly looking at legislation like (CalEPA) or the CCPA in California, it's that definitions are great for lawyers to figure out ways to circumvent. So if you really want to solve the problem, you need more of the sort of solution -- again, Peter's been talking about it -- that the Europeans have approached in dealing with privacy. Part of the reason, if I can answer the question to Peter, that we haven't had that answers it's because the FCC hasn't (inaudible). They're not a privacy organization. They are in an enforcement action against carriers for their misuse of location data. They own the statute. They could have published immediately a limitation on or explanation of the use of location information, or the disclosure of it by carriers. And they haven't done that. So we sort of live in that different world, and the definitions we're getting in legislation today are both too general and too easily circumvented to be meaningful. And so I think we need a much better discussion on what the horizontal answer looks like instead of the vertical answer for each type of provider and each type of technology. It would be better in this case to have a very clean, clear explanation of what can be done with location information and when.

DANIEL CASTRO:

(51:07)
So the next question. I'll let whoever wants to take this one take it. What's the difference between anonymizing and (pseudo) anonymizing data? To what extent is aggregated data or anonymous data sufficient as a privacy safeguard? Peter, maybe I can point that one to you.

PETER MICEK:

(51:28)
All these terms are very loaded, and again, there's like big commercial interests pushing the idea that you can de-identify data or aggregate and anonymize. There are methods to disassociate data from the person or the entity or the location was collected from. A statement from Vodafone's CEO today recently talking about highly aggregated data, which something of that does sound scientific. I think it's safest to say that, by default, no data is anonymous. Start from that as the basis. It's very difficult, especially when using cross-reference datasets, and the more data that's out there, the more that's flooding in the marketplace and being shared (it makes it) more likely that some third party is going to get hold of different data sets and start to cross-reference them and de-deidentify to draw insights from that. So that's another reason we want really demand a more targeted sense of what should be shared. We don't want to leave it up to the companies because, if they can push some data set right now as de-identified or as

aggregate anonymous and safe to share, you can bet they're going to use those same arguments two-three years from now to say why it's okay to share with potential advertisers or data brokers or why they should be exempt from certain data protection provisions. So, I'm sure Rachel and others have thoughts on that.

DANIEL CASTRO:

(53:29)
Thank you. Yeah. Rachel, did you want to weigh in?

RACHEL LEVINSON-WALDMAN:

(53:32)
Yeah, I take all Peter's points. I think really the only thing I would say about sort of pseudonymized versus anonymized, I would sort of think of those in terms of there being a distinction. And I think it's really right that one of the things you need to think about is sort of how different data sets could be correlated with each other to identify even data that seems quite anonymized. I guess I would think of the distinction as pseudonymized data is data from which identifying information has been stripped, but there is still enough information there to put it back whether it's through analysis of that data set or combining other datasets. Truly anonymized data at some point is always going to be identifiable, right? But if a company said, we have seen based on our data -- especially if you have a large enough set-- that 2,000 people from the neighborhood that I live in went downtown yesterday (so people in your neighborhood, please don't be doing that unless you really have to), I don't think that's re-identifiable. The company can identify. They're the ones who started with this data and presumably they're pulling from whether it's mobile phone data, advertise your data, something like that. I think depending on how it's being shared out, you could imagine datasets at the very least for, sort of, for public education, that as far as the public is seeing it really aren't identifiable. Again, if you have enough people. You say, two people from your neighborhood went downtown. Then maybe actually somebody could figure out who those are if you're in the neighborhood and you can talk to people. And (a large enough said), I don't think that you're identifying it. And I think this also relates a little bit to the point that I was making about on the one hand sort of privacy advocates say that location data, phone data is too precise and now we're saying it's not precise enough. I do think those two can coexist, right? It is quite precise if you're talking about patterns of movement, where are people going, what house are they at. You know, are they joining a rally? Are they going to an abortion provider? Things like that. Which is different from I think being able to know for every one of those points were they literally sitting outside or in the waiting room or inside an examination

room that's right next to the waiting room. There may be some kinds of technology that are precise at that granular level, but some that really won't.

DANIEL CASTRO:

(56:05)
Thanks. And so last question I have here really just to wrap up. You know, for lawmakers who are wondering what else they can do in response to this crisis or be better prepared for the next one. In terms of balancing privacy and access to data, what's your main message? We can do Peter, Rachel, and then Al.

PETER MICEK:

(56:30)
The main message to policymakers: we want things to be above board, to be transparent, and to involve the public by default. And you know, (same as) a civil society group. But, I think the idea here is that the more eyes we have on the next steps, the better it'll be, the faster it'll roll out. When it comes to respecting digital rights and human rights. we have some red lines in our paper, again, that's up on our website AccessNow.org. We don't want to see this as an excuse to roll out untested and dangerous technologies like facial recognition. We have a lot of concerns about the mandatory apps that a lot of countries are forcing people to download. Again, untested technologies that probably are very (weak), and (easy) to be exploited. And so, you know, I think, we want to urge caution, and urge policymakers to do things out in the open as much as possible, to have really targeted and purposeful, and informed, interventions that do take place on a legal basis and within a respect for human rights.

DANIEL CASTRO:

(57:52)
Thanks, Peter. Rachel, anything for lawmakers especially as they consider maybe another stimulus bill and (inaudible) targeted bill of the coronavirus crisis.

RACHEL LEVINSON-WALDMAN:

(58:03)
Yeah. And then I guess, not thinking so much about the stimulus bill, but sort of generally what lawmakers should have in mind. I mean, you know, I think by and large, I would agree with Peter's points. And I guess just generally, I would say, bring in expertise, right? So that's public health expertise, that's privacy and civil liberties expertise, that's civil rights expertise, that's

technological expertise. There's a lot that's unknown and a lot I think that everyone is figuring out. And I think bringing people to the table who have real expertise and insights will help to facilitate all of the things that we're talking about in terms of making thoughtful decisions, having transparency, putting restrictions on, things like that.

AL GIDARI:

(58:46)
I would second my colleagues' comments. I think they're all good, but if you really want to unleash innovation in the tech sector to address problems like pandemics and that scale, you need to eliminate the fear of the long tail of the data. And so if you could do anything by (inaudible) HHS, FCC, they could immediately solve this problem of the fear by prohibiting any secondary use of the data outside the public health administration and removing that fear would go a long way to building trust. And if people can trust, they'll share. And if they share, we can solve the problem much more efficiently. I think we live in a world of fear because of our past history on this. And, you know, no one is doing anything in government to clean that fear up. And I think it really is the critical issue to solve how technology can aid in an emergency like this.

DANIEL CASTRO:

(59:51)
Great. Well, thank you. Thanks to everyone who joined us today. Thanks to the excellent panel for this conversation. I think this is a conversation that we're going to be continuing to have in the weeks ahead and probably in the years ahead as well, so stay tuned for more on this. Again, thanks for everyone for joining us today and have a good Wednesday. Stay safe and healthy.