COVID-19 Contact Tracing Apps in the US, EU and Asia

Wed, June 10 2020

Sabine Muscat
Welcome everyone to our online discussion today on digital contact tracing in the US, the EU and Asia. My name is Sabina Moscato. I'm the program director for technology and digital policy at Heinrich Böll Foundation in Washington DC. We are very proud to jointly host this event today with the Center for Democracy and Technology. for them. It's actually the third installment of their webinar series on tech policy responses to COVID-19. And if you haven't seen the previous two, they're on their website as well. For us, it is the inaugural event of our own online event series on tech and COVID-19. And the series is based loosely based on a series of articles that we've been publishing as a joint project between our offices in Washington, DC, Hong Kong and Brussels. So it's a very global project and a very global cooperation. So you will find these articles on our websites in Brussels and Washington DC. So more content is coming. Stay tuned before we start this event, I wanted to remind everybody to just announce that this event will be live streamed on the CDT website and it will also be recorded. So this is live and will be recorded. In this session we'll talk about digital contact tracing approaches around the world. And I would like to first start by introducing our panelists from three timezones. First, I'd like to introduce Greg Nojeim. He's the director of the freedom security and technology project at CDT. And he'll give an overview of approaches on contact tracing in the United States from the technology that's based on the Apple Google API all the way to other tools that are being used at state level. Dev Lewis is joining us from Shanghai and he is the fellow and program lead at the Digital Asia hub, and he'll talk about lessons learned from Singapore's TraceTogether app, but he will also compare it to some more intrusive approaches across Asia, for example, India's Aarogya Setu app or he will also tell us whether or not China's health code is actually a contact tracing app or not. Then we have Frederike Kaltheuner. She is a tech policy fellow at the Mozilla Foundation. Some of you may know her from her previous job, working for Privacy International. And in the UK. And Frederike will give an overview over apps that are currently being introduced or delayed in European countries such as Germany, France and the UK. And in two of these countries, the governments have decided that they will not use the Google Apple API, and Frederike will explain what that means.

Sabine Muscat
So before I give the words to our panelists, let me give you a quick overview of our topic. I mean, I know that many in the audience I experts on the issues already, so I'll keep it brief. What is contact

tracing during an epidemic, it means that health authorities reach out to people who have been confirmed as infected typically by phone with the goal to verify and identify their contacts. The next step is then to notify these contacts and to determine how long they should self isolate based on proximity and duration of exposure. And, of course, most countries that were able to contain or slow the spread of the virus Also, we're very good at other aspects of this and in terms of testing, or in terms of enforcing social distancing. So contact tracing is just one element of epidemic control. But what is digital contact tracing? The hope now is, of course, that digital technologies can supplement manual contact tracing, and many countries are introducing apps that can send notifications to people who've been exposed. But can this be done in a way that is both effective and protective of personal data, and this is what we're trying to discuss. We're seeing a whole scale of more and less privacy intrusive approaches around the world and even within countries right now. So just to name the most important divisions here, the most important device some apps, track, GPS location data, other apps don't They just record a digital handshake via Bluetooth, low energy technology. And that means that if I, if my phone meets your phone and I get infected, and my phone will send a notification to your phone later that you've been in proximity with me, there is a debate over a centralized versus decentralized storage. Should the data be stored at a central government or public health location? Or should they just remain on the user's individual's phones? There is debates about the duration of storage, how long should this data be stored? If they're stored, when should they be deleted? Should these apps self destroy after the epidemic is over? There's questions about data access by public health authorities should they have access to the data or not and in which format? There is a debate about whether participation in these acts should be mandatory or voluntary. And there was also a lot of apps that are hybrids. I want to say they do contact tracing but they also do some other things as well. They have add ons, if you will, for a symptom tracking or voluntary data donation, whatever. So our speakers will talk about where they are regions stand on the scale from most intrusive to least intrusive or to privacy protecting and what the experience are that they're making. So the speakers will talk for about 25 minutes. After that, I will moderate a short discussion with the speakers and then we plan to leave 20 minutes to take questions from the audience. If you do have a question, please submit it through the Q&A at the bottom of your screen. And it would be nice if you could in that when you type in your question also identify who you are and your organization. However, if you wish to remain anonymous, that is also a possibility, but then you should also let us know so we do not by accident, mentioned your name then when we take the question, my colleague called Roberts, our head of communications will moderate the questions from the audience at the end of the session. With that, I'd like to hand over to my co host, Greg, who will explain what whether us is at and what Google and Apple are doing. Thank you.

Greg Nojeim

Thanks Sabine. I really appreciate the opportunity to be here. And it's a pleasure to co host this with the Böll Foundation. Center for democracy and technology, my organization, is a nonprofit organization. We're based in Washington DC, we have an office in Brussels. And as you mentioned, this is the third in our webinar series on COVID-19. And technology. The first webinar we did was an expose of the gaps in US privacy law laid bare by the US reaction to COVID-19. The second in our series was a debate on contact tracing apps, Bluetooth enabled, contact tracing apps, and this is the third. To see the others and to see this one and the recorded version, go to our website www.cdt.org I'm going to build a little bit on what Sabine said about how these applications work. And then I'm going to discuss

the Google Apple API and the Bluetooth enabled apps that they envision and that they are helping to enable. And then I'm going to talk about the situation here in the US and then turn over the mic. So as Sabine said, these applications are designed to assist with contact tracing, which is really an art. It's the art of building trust with a person who has been infected with a disease that could be life threatening, and building enough trust so that that person feels comfortable disclosing their contacts so that those contacts can be notified that they may have been exposed to the virus and need to be tested or to self-quarantine. It takes a lot of trust in the manual world to do this. And it takes a lot of time. A person who is affected may not remember all of the contexts that they've had. They may not know the names of people with whom they were close for a period of time, perhaps in a restaurant or in another building an office setting, even. And they also need information about what to do next. You know, you don't want to have a person get notified that they may have been infected and then not be given information about what to do next. And digital contact tracing is seen is seen as a way to facilitate the manual contact tracing. In other words, it takes away part of the time needed to give notice to people that they may have been exposed and it's makes it so that that notice can be given more efficiently and more quickly. And speed is of the essence in fighting COVID-19. Because people who are infected often have no symptoms. They don't know that they have to limit their contacts. So it's really important that context get noticed quickly and efficiently. The apps that Google and Apple are facilitating through an API are Bluetooth enabled apps. Bluetooth is a radio signal. It's the thing that passes from your computer, to your earbuds or to your speakerphone or to your speakers. That makes it so that the two can talk to each other. The Bluetooth signal was not designed for this purpose. But it is being used for this purpose in Apps around the world.

Greg Nojeim
As Google and Apple have designed it, it will work like this. Two people download a Bluetooth enabled app. If they spend more than a few minutes together, their phones exchange anonymized IDs. And those anonymized IDs are stored on each other's phones. If one of them becomes infected, she triggers a notice that is sent of a notice of possible contagion. That is sent to all of her contacts all of the people whose phones registered on her phone. As designed by Google and Apple, the system has important privacy protections. It's voluntary. In other words, you can't that government can't be compelling you to download the app. It's voluntary in another way to in that when you become diagnosed with COVID-19. You receive the information that you would need to give notice to your contacts that they may have been exposed to you. And you receive that information from a health authority. You then have to act to give notice. In other words, there's two voluntary points, downloading the app. And then the action of giving notice to people with whom you may have had contact. The notice is anonymous in a sense that once it is given the people with whom you had contact who get the notice, they don't know who their contact was, that triggered the notice, and it was affected. And that's an important privacy protection as well. The system is decentralized. That means that the randomized IDs reside on the phone of each user and not on a central government server. And importantly, no location information can be collected. location information can be very revealing about one's activities in the United States. location information is being given legal protection akin to that, given the contents of communications. An app based on the Google Apple application program has to have these features. If it doesn't, it gets denied access to the API, and it won't be able to work. There are limitations on this system. And there are a lot of concerns that it may not be effective. First, there has to be a lot of uptake. That means that if the person with whom you're close in proximation, close proximity to for a

lengthy period of time has not downloaded the app. That person will not get notice, even if you have so both people have to download the app you both have to participate. It's voluntary, in the sense that a person could decide not to give notice, once they've been diagnosed, that can decrease the effectiveness of the app as well, it relies on two variables, duration of contact, and Bluetooth signal strength. Bluetooth signal strength goes down, when the distance between the two phones increases. That's a good thing you wouldn't want to get notice and an extremely weak signal, because that might mean that you're not close to a person close enough to have been too big to have become infected. But signal strength can also be decreased by other things. For example, the orientation of the phone might might impact signal strength, is it like this as compared to the other phone or is it like this? So the orientation of the phone makes a difference, whether the signal has to pass through clothing through a wall through a person's body, because for example, two people are in conversation with each other close but they both have their phones in their hip pockets, that would decrease signal strength as well. So it's an imperfect measure. And we're not sure that the system will be in fact will be effective. One more thing to consider is interoperability. Google and Apple can't guarantee can't make it. So the different apps that are being developed to use their API are interoperable with each other. interoperability is key because people move around. For example, I live just outside of Washington, DC. If my jurisdiction Maryland, adopts one app that isn't interoperable with the app that Washington adopts, then we'll have a problem because I won't get notices of potential contagion.

Greg Nojeim
In the US, the fight against COVID-19 is conducted mostly at the state and local level. That means that local health departments will be developing these apps or hiring developers To develop these apps, a number dozens are in the works that will rely on the Google Apple API. None have yet been released. three states have released apps, at least three states have released apps that do not rely on the Google Apple API. Those states are North and South Dakota and Utah. The North and South Dakota app relies on location information, not Bluetooth information. And the care 19 app which North Dakota, South Dakota us actually violates its own privacy policy, because it shares location information to the government. Not a good start. So we're waiting for the Google applet API's I'm sorry, apps to start coming out. And we'll revisit this issue when they do. Thanks much debate.

Sabine Muscat
Great. Thank you very much, Greg, for giving us also a bit of a technical overview of how this works that's very important for everything we're going to discuss today. And with that, I would like to hand it over to Dev in Asia has been making Asia was the first continent that made experiences with these apps. And I think a lot of our apps are now in some way shape or form being modeled on Singapore's app, the trace together app. And yeah, so we are curious to hear from you. What How does this work in Singapore? And what other approaches are countries taking in Asia? Thank you.

Dev Lewis
Thank you very much, Sabine, and Hello, everyone joining from around the world. I believe my video, you know, we don't have access yet.

Sabine Muscat
But we can hear you fine. Oh, there you are. Great.

Dev Lewis
And yeah, thank you so much for organizing this excellent event. And Greg's initial remarks really explained the sort of the designs of contact racing apps. And it's a, you know, it's real, it's very 2020, right? That we're sort of in the middle of a pandemic, and we're talking about an app, or many apps and different types of apps. And, you know, we've been using apps for to solve every problem for the last few years, rightly or wrongly. And here we are, again, in this pandemic. And you know, I've been sitting here in Shanghai since the start of the pandemic, and it's really been technology has been such an integral part to life here. From every aspect of going out, travel from finding out your environment, what's available, what's open, what access you can, you have available. And so it's been really interesting to observe what different countries in Asia have done. Since time is limited. What I will do is I'll quickly give a brief on Singapore and what Singapore is done with its TraceTogether app, followed by some examples from South Korea and China. And really my core thesis that I think I want to make. And Greg touched on this in the end of his talk was that we don't really know if contact racing apps work. And my observation so from Asia tell me that contact racing apps do not work ,and by far are lower in priority of what needs to be done both in the technology interventions at work, as well as non technology interventions. To Singapore, as we all know, was one of the first countries on March 14 came up with an app called TraceTogether using a new protocol called Blue Trace, which is very similar to what the protocol that Apple and Google have now developed that Greg explained, as well as what Europe and the EU has, has developed as well. And Singapore to start, you know, was this perfect city state, a very technology driven government, and this app became this idea that you know, this will be the solution for us the right to the pandemic, you got this app, right? And now we're gonna, it's gonna cost your life. And you know, we'll get messages when I have a close contact, and I'll stay home if I need to. And we'll go about life as normal.

Dev Lewis
But I think what we've seen in Singapore could very clearly is that TraceTogether has not worked. Even in the sort of tech utopian city that is Singapore adoption was on has not crossed 25%, which is very low, very low threshold from the somewhere between 50 and 60%, that experts say is needed for contact racing have to have some significant impact, even though the app plays privacy very, sort of at the center of its design, just as we're seeing with with the Apple and Google examples. The key point is that the actual efficiency of this app is really low. And you know, we saw over the course of April, Singapore actually go back into a very strict circuit locker that they call, which essentially was a sort of tacit admission that contact tracing apps just haven't worked in the desired effect. And one of the big reasons is that, you know, you had large communities, we didn't have the app. And we had, you know, migrant workers in some dorms. And you had a big spreading event going on going on there. And then since then, we've seen Singapore sort of go back into a lockdown mode. And recently some of the examples coming in Singapore, I think, also show that really the contact tracing apps is such a small part of the overall tech interventions taking place. We saw on 12th of May, Singapore introduced something called the Safe Entry, which essentially works as a way of location logging. So people who enter malls and hospitals and large public venues, they scan a QR code using either the Singapore SingPass, which is a very popular app in Singapore or using the National ID and they basically log their entry and exit into these various locations. Singapore also introduced Bluetooth tokens, which are essentially wearables, that act like contact tracing apps, but they're not apps, they are physical

wearable, which you carry around. And I think these have largely shown that, you know, despite Singapore's high digital literacy, despite the high adoption of apps, and Internet penetration, contact tracing apps have just not cut it. My observations from looking at maybe some of the other countries that have had some success in COVID, cutting the spread, is maybe South Korea, and South Korea is notable for not having a contact tracing app, specifically. They make use of apps in a whole host of ways, from enforcing quarantine very strictly using GPS data, and using telecom data to make sure, especially in March and early April, when you had a huge influx of global foreign travelers, and they were coming back into South Korea, and to sort of make sure that they stayed home. This was a very cool part of of a lot of the measures taken also in Taiwan, in China, and in many countries in Asia. And I think that has so far played a much bigger role, so far. We've seen some excellent research coming out from researchers like Hatsuku (?) in South Korea, who've shown that building a, they've been able to use data towards assisting contact tracing apps, sorry, to do this assisting manual contact tracing without relying on apps. So they built a large database that takes in various kinds of data, mainly Telecom, immigration, financial data transmitted and medical records. And what this has done is basically created a way for manual contact tracing to happen really fast happen before let's just say the spread can go much further. to essentially catch all the contacts, all the close contacts within two to three day period, before they start showing symptoms. And, you know, South Korea's methods have been, have also faced a lot of criticism within the country, thanks to the emergency laws through the 2015 MERS pandemic, the government has been able to sort of bypass its very strict privacy laws and create this large database. There's been issues over disclosure of personal information to the public, which has happened a lot of times, and then on June 10, very recently, South Korea has also brought in the QR code system, which is what similar to what Singapore is doing now, which is again logging people's entry and exit into these key areas where there's high transit people, essentially to say, Okay, if there's someone found here, you know, we can trace it. And as we've learned also from that, I admit, there's a lot we don't know about this about COVID-19 and its spread, but largely data shown that you know, spread can take place and where people are in close proximity mainly indoors and for a sustained period of time. And so if you can sort of narrow those are the kind of places the kind of venues where people have that kind of activity, whether it's churches, whether it's in malls and shops, and you can narrow it down, you can assist your manual conduct research without relying on apps. And finally, to the big question about also China's QR code I've seen, you know, I've seen a lot of writing about the China's health code being a contact tracing app. I think once you really closely look at it, you find out that it's really not, you know, China had an opportunity, you would think, in February to build that. But looking at the way it functions essentially it's a health passport. And the data that it relies on is not from anything that it is obtained from your phone. That data comes mainly from government public data records, medical data from also from telecom data. And essentially, it's become the sort of pass to ensure and to manage which, which people can travel, which people can access areas that are considered high risk. And so to end my remarks, I'll just say once again, emphasize that. So far from what we've seen across Asia, there are over 10 countries that have contact tracing or COVID apps. data so far suggests that contact tracing apps are really not what they made out to be. But they play a role. And I think that should become a part of the discussion going forward. And I'll yield the floor back to Sabine and I hope to just continue the discussion over the next half an hour. Thank you.

Sabine Muscat
Thank you very much Dev. And thanks for the overview of Asia here. That didn't sound like very promising for us in the other parts of the world who are just about to introduce these apps, but it's definitely lessons we can learn from in some ways, in some ways, we probably can't because of other different understandings of privacy and so forth. So, with that, I would hand it over to Frederike. And she will talk about Europe where apps are currently being released. And it's rather confusing because every country is using a different approach here. But of course, in Europe, everybody has to abide by the general data protection regulation GDPR. And how that works. I'm curious to hear that Frederike.

Frederike Kaltheuner
Thank you very much, Sabine. I think my video is also still turned off, but I can just start. I just want to say I in the past few months, there have been a lot of discussions, especially in Europe, about contact tracing apps. And there was a point in time when I felt quite uncomfortable about this, because I felt the amount of discussion dedicated to this to these apps stands in proportion to the role they actually play. And I have to follow what epidemiologists say who all sort of seem to express that they could potentially play a part. But they're always one piece of the puzzle. So there's been a lot of conversation in the tech community of the contact tracing app. And I also want to reiterate to say that the concept comes from epidemiology, and I don't feel comfortable to assess, or even judge if they are useful and I think we need to trust the assessment of scientists there. Something that's also kind of important in normal times, contact tracing apps, by definition, are an incredibly invasive technology. In normal times, it would be unthinkable that governments introduced introduce such an app, which means that sort of like following the human rights standards for privacy, all of these apps need to meet at least three kinds of criteria, which is they need to be lawful. They need to be necessary and they need to be proportionate. All of these apps come with a number of assumptions. They assume that people have a phone Then they have a phone on their own. This is not always a given. They assume that people can get tested. I'll talk a little bit more about this later. And they assume that people can take necessary actions, which is to isolate when they need to. And that's also not a given for everyone. A lot of the focus has been on privacy and security. And I want to add that this is just one aspect. Another really important aspect is justice, inclusivity and equity of these apps. So who can use these apps? Poor people or who people can't afford expensive phones often use phones that run on older versions of Android? And that's been a huge issue in several countries. Another question is what happens if you don't use the app? What happens if you don't have a phone? Is there the risk for function creep? So those are aspects and the fault lines that exists within Europe. They're not just between centralized and decentralized. They're also about other things. They're also about what role should testing play should people be allowed to self diagnose on the app through a questionnaire? And if they get a test? How do they input the test results? So there are very different approaches in Europe. Before I go to France, Germany and the UK to explain a little bit what's happening over the past few weeks the overall impression from Europe and I wrote a piece about this with my friend and colleague Corinne Cath-Speth from the Oxford Internet Institute. The European approach has been very fragmented, which is actually quite remarkable given that if we believe epidemiologists who say that this app plays an important role in reopening and especially in reopening European borders, it's quite remarkable that not all of these apps were initially interoperable. Meaning that if a French person travels to France or somebody who lives in France travels to the UK, the apps don't necessarily communicate with each other. Since we wrote that article, a lot of things have changed a little bit. There's a tendency now, still the UK and France have created

apps based on the centralized design. So they're not using the API developed by Google and Apple, more in the UK, but later. So these two apps as they stand, they're not interoperable with other countries. But at the same time, we now have Austria, Latvia, the Czech Republic, Switzerland, Estonia, Italy, Germany, and until two days ago now also Poland, who have either released an app that's based on the Google Apple API, or are planning to do so.

Frederike Kaltheuner
So, now a few notes after this overview about France and I can't move my notes, oh yeah I can. A few notes about France. So France launched their app on the second of June this week after intense debate. France is not relying on the Google and Apple contact tracing API. They've instead are relying on a different protocol. This is a variety of something that's been discussed at the PEPP-PT protocol. So they're relying on a protocol that has been designed by French and German researchers. And that's also a version of the protocols, also in Germany initially wanted to use. So it's been only been a week. So it's hard to say to make an initial assessment of how the app work. But what's important is it does work different from from the decentralized apps, and the key difference is -- It also uses Bluetooth -- But a key difference is, after a diagnosis, either by a doctor in a hospital or by testing facilities, people get handed a QR code that the app scans. The centralized component is that all contacts that somebody has been in contact with will be uploaded to a central server. So this has been heavily criticized in France. There were letters by hundreds of researchers warning that this is invasive. But ultimately, parliament voted in favor of the centralized approach. And just to repeat, so the French app is not interoperable with the apps used in other countries. Germany changed course in late April, which was interesting. This happened very last minute over a weekend, I think. So they abandoned the homegrown alternative and and are also using the API developed by Apple and Google. The app has not been released yet, but it is about to be released soon. Researchers have seen the source code and have found no trackers or obvious security flaws until now. So this uses sort of the different slightly different protocols the DP-3T, those are also group of European researchers who developed a decentralized approach to contact tracking, and uses no location data. There's no centralized storage of data, so only a pseudonymous or anonymous list will be stored centrally, but there will be no matches made on a centralized server. And that's a difference to France. Concerns about the German app are, so one question is it also relies on a QR code, and the British one does not. Which means then once you get tested, you will be handed a QR code that you can then use the app to scan. The question, or an open question, is whether labs and the facilities that that do the tests will be able to produce these QR codes. That's something that is unclear. It's also not clear, and I checked this again, two days ago, there has not been a comment by the developers about interoperability. So using the Google Apple API means that it's possible to be interoperable. But still the different national servers need to communicate with each other. So this is still an open question.

Frederike Kaltheuner
What I thought was very interesting is that it really seems that Germany changed course after heavy pressure from civil societies, specifically, and a few more notes in the UK, a summary of the UK approach and I'm very much looking forward to writing a longer piece with (?) foundation on the UK specifically, I'm not exaggerating when I say this is a really good example for how not to use technology in a pandemic. So the UK has started the trial of a contact tracing app in May. And there have been severe problems. So analysis by Privacy International found trackers in the app, that's absolutely a no

go in any health app. There have been wide ranging security flaws detected, residents in the trial have had problems using the app. And I think generally, the way this was communicated has, has resulted in huge issues of trust. So there were unsecure documents found on a Google Drive that indicated future uses of the app that hadn't been communicated. So, for immunity passports, location data. At the moment, there's no launch date for the app. And yesterday, there were notes that the Prime Minister is also now pushing for an app that's based on the Google Apple API. Something that happened in the UK that didn't happen in other European countries, or that hasn't really been debated in the same way. And I was thought it was interesting that Jeff mentioned this as well. The UK is developing something called a track and trace scheme. So this is the technology and data infrastructure that supports its manual contact tracing operation. But the government is currently being sued over this track and trace scheme, because it failed to meet GDPR requirements. It had an insufficient privacy notice, there was data retention for 20 years, which was the sort of, which led to the legal challenge that we've now seen. So I think a summary of the European approaches, it's been, it's been very fragmented early on. And I think it's not sort of, that's not a, the pandemic was the trigger, but there are some underlying tensions that have been present all along. One scene that happened quite early on Is that governments like France portrayed their attempts or like frame their attempt to build a more centralized app as sort of a standoff between Silicon Valley on the one hand and the French government on the other hand, and it is true from a European perspective, it is quite remarkable that Apple and Google can de facto dictate how European governments build their contact tracing apps. Something I didn't mention, and do interrupt me when my time is up. Something I did mention that the problem of, that countries like France face, is that if they do not use the Apple Google protocol, the way they have to rely on the usual Bluetooth API, and what that means is that for good privacy reasons, you're not allowed to run Bluetooth in background, so apps can, especially on like on iPhone, this is an iPhone problem. So you can't use, have Bluetooth turned on, when the app isn't in the foreground. So the moment you close the app, the moment the phone isn't fully on, Bluetooth is not connected, which means that you could very well be in contact with someone who ends up testing positive. But the app doesn't record this. And France framed this as we need Apple to cooperate, we need them to change the API and give us allow us to build the contact tracing app we want. But the perspective from Apple's side was, we cannot sort of, like we opened the floodgates for very invasive commercial apps that could also be using this API. So that was the theme, this being framed as a standoff in Germany as well. And also sort of in the UK press. It's called Are we're using our own NHS app or the Google Apple App? even though this is strictly an API. And in the piece I mentioned that I wrote with a colleague we sort of concluded to say, yes, it is remarkable. And this is a reminder that that Google and Apple have an extraordinary market power when it comes to mobile phones, and this is something Europe is challenging. But, at this moment in time, they happen to be they happen to be supporting the most privacy friendly and the most, the most privacy friendly version for contact tracing. So they're sort of trying to preempt more invasive governments from developing more invasive apps.

Sabine Muscat
Thank you Frederike. I think. This is exactly actually where I would like to start the discussion with you. Where you ended your presentation was very good overview over what's going on in Europe and difficult debates countries are having about this. I mean, Germany's back and forth on this was rather epic. We had a piece on that in our series as well. And, in the end, it's really the question. So we're having a global pandemic, but we're having national solutions. And not even liberal democracies,

among each other, not even EU countries among each other, were able to find a unified approach, and instead, it was actually, it seems like Google and Apple, the big tech companies are ending up setting the universal standards for this, in some way or other, even though not all would, would really adopt it. But I would also like to hear from the other two speakers, what does this cacophony that's surrounding these apps actually mean? And what does it mean for standard setting in global digital governance, that nobody can agree on something that's actually a rather simple, perhaps temporary, if you will, technology? So I think I see all of the screens are open now. Greg, would you like to say something about that?

Greg Nojeim
You know, I just this kind of thing shouldn't be surprising to us. It's a global pandemic. And, to some degree, the lack of organization isn't always a bad thing because sometimes one can become organized around very privacy invasive approaches. I do find it interesting, though, that Google and Apple have built in privacy protections that some governments are saying are the wrong judgments. Now, they may be right. But I think that because of the legitimate concerns about the degree to which these apps are going to be effective, that we ought to be taking a very privacy protective approach. Because you wouldn't want something out there that a lot of people use that turns out not to work and that invades their privacy. I think we need to head that possibility off.

Sabine Muscat
Dev, did you want to comment on this or is in your region the Google Apple API will not be such an issue? Which coverage Asian countries are even using it?

Dev Lewis
So far, none. We've seen about nine countries come up with their own versions of the contact tracing app. And none of them use the Google Apple API. But, from what speaking to some researchers who are working closely with governments in Southeast Asia, essentially what is happening is they all have countries waiting for more information. And so I think we might see some adoption, especially over countries that have not integrated contact tracing apps right now, about maybe four or five countries in Southeast Asia. Right now, India's the only South Asian country to use a contact tracing app, Aarogya Setu. So, we have yet to see what the rest of South Asia does. So, for sure, given the adoption rates of the Android ecosystem in this region, absolutely. I think that protocol will be erupting and bringing up new questions to the fore. There's some great questions in the q&a. And maybe I can sort of touch on some of them.

Sabine Muscat
Dev, actually, Carl is going to moderate the q&a in just a little bit. But I have one last question. And then we can immediately go to the q&a, but that's actually to you Dev as well. And that would be when you said, well, China considered it not useful to use a Bluetooth tracing and all that. And they didn't think that they needed even location data for this, and therefore they needed other types of data. And many, I think governments might agree with that, even if they're, even if they're democracies. On the other hand, with China, we know that they already have all the location data, right? They have everything they need to have. So, it's a very different premise in some ways, and but I do know that there are lots of desires from Western governments. I know that Frederike said, the British app, for

example, also wants to include a symptom tracking function, and in Germany, there was a lot of debate over data, voluntary data donation, health data donation. So is this a slippery slope? Do you think when governments feel like these apps are not doing enough, that we are going to move towards, we will find more appetites towards an Asian style, bio-surveillance as you've called it in your article, dev?

Dev Lewis
Yeah, I mean, I think it's always difficult to make straight comparisons between countries in Asia and Europe, or even the US. You know, there's so many different legal regimes, just cultural attitudes, which are to be honest, not always correct, for example, like I think we tend to overestimate how much data the Chinese government has access to. And often more times than not, they actually, you know, would dream of the kind of access that I think some of the reports ascribe them to having, and I think with this, with the health code, I think what's interesting is that we've seen the adoption at unprecedented levels. 900 million people using them. And, as for data that we have released as of early May, one, each person has used it eight times. That's pretty astounding figures. And I think what, that has basically now laying the groundwork in China, this is now what the concerns are with privacy is, what happens next? You know, when is the staff going off? When did the lights go off? When does the, you know what's going to happen next? And we've seen concerns happen already. So, there was a lot of manual data collection happening through February and March, pen paper, writing contact numbers and ID numbers. And so you had a lot of rise in cybercrime and phone (?) happening with, you know, this information being leaked because you don't have strong data protection standards and protocols for data collectors to follow. And now what's happening is because this health code is in everyone's phone, government, the Chinese government is saying that wow, we have this app. Everyone's using it. Can we do more things with it? Can this become a gateway towards, you know, e-healthcare? And the same thing's happening in India as well? Basically, you have like, now we have this infrastructure. Now we have people who are building the habit of using it. Can we do more with it? And to be completely objective and balanced, healthcare in both these countries are broken. And, absolutely, governments need to be doing more for health care. But the problem is, is that there's no protocol right now for how to manage the store of data. There's no, there's no clear protocol for what happens to the data. When the pandemic's over, they say some of the data can be deleted, but there's no real, there's no official answer. And that's what is actually causing a lot of alarm right now in the region.

Sabine Muscat
Thank you, Dev. I think Frederike wanted to weigh in on this one real quick, and then we'll definitely have to get to the audience questions because we have a lot of them, I can see. Okay.

Frederike Kaltheuner
I have like, I'll just say a tiny bit, I want to say that we always say in Europe we have the GDPR, but governments can use, rely on, surveillance powers to use data in a pandemic as well. And this is something that's been a little overlooked when we say, well, we have GDPR, there's not going to be a problem. But the UK example also shows the software the UK Government is using for manual contact tracing has been developed in cooperation with Amazon, Palantir, which is a controversial company, to say the least. Google has also been involved. In the lawsuit that's filed against them is also there have been so many questions, what are the agreements? What are the data sharing agreements? Can these

companies use these data to train AI? So even with GDPR, there remain many concerns. So we proposed a regulation on contact tracing to make sure, basically, it needs additional law in Europe as well, to make sure that there is no function creep.

Sabine Muscat
Thank you Frederike and with that, I'll hand it over to Carlin spin. Going through all the questions that came in is Hi, everyone.

Carl Roberts
My name is Carl Roberts, and I'll be moderating the audience q&a part of the portion of this presentation today. So, I think we'll just jump right in. I'd also like to apologize in advance if I mispronounce anyone's names. I'm sure I will do that. So please, bear with me. The first question we're going to take is from Judith Bayer. And this is for all three of our panelists. I think. After a person enters for positive test results in the app, what prevents her being labeled in real time, does the app give a signal to other nearby apps that have COVID positive person is near them. Wouldn't that be desirable but also catastrophic to privacy?

Greg Nojeim
May I start? I think it would be catastrophic to privacy. I don't think anyone would use that app, right. If an app is catastrophic to privacy, it's not going to be used, unless mandated, and even if mandated, it's not going to be used. People won't, people will find a way around it. So, the way it actually works is, or the way Google Apple contemplate that it works is, your phone is always generating an ID that changes every 10 to 20 minutes. And that ID is registered on other people's phones who are near you who have also downloaded the app. And so when one of those people so say you are diagnosed with COVID-19, those people who you were near for the period of time that is seen as epidemiologically significant, they will get a notice when you insert the code that is necessary to trigger the notice. That's the theory of how these work. They won't know that you are the person to whom they were exposed. They won't know when that exposure happened. They won't know for how long they were near that person, they'll just get a notice saying, hey, you may have been exposed to COVID-19, you probably ought to get tested, or you probably ought to self-quarantine. So, there's not this real time notice to the people around you, that you got COVID-19. That's not how these will work. Thank God.

Dev Lewis
It happened in South Korea, and it was not very welcome.

Carl Roberts
So I think that answers that pretty effectively. We've got another question. From Pienaar bar loss for those of us in countries that are just now starting to develop their apps. What kind of concerns can we bring to the developers or government? What kind of features and considerations can we demand that make the app respect privacy rights and still remain effective? And I think this is again for all three of you.

Greg Nojeim
Frederike, why don't you start?

Frederike Kaltheuner
So I think the bill that I provided some input in for the UK is a really good framework. There are a lot of organizations to develop sort of what's a list of criteria that these apps needs. I think the first one, and as we learn more about how other apps in different countries are working, is to be it needs to be, the effectiveness needs to be evidence based. And this needs to be continuously evaluated. We can't just in app one, solve the pandemic. We all know this. If it plays a small part, we need to monitor how effectively that happens. There are good principles in data protection, data minimization, purpose, limitation, transparency, fairness, that are just good design principles for building any technology. The number one important thing is this app has to be strictly voluntary. And I think what's so important about this is that this also means that if the app isn't trustworthy, people are not going to use it. So it puts an additional pressure on governments to build an app that is worthy of people's trust. And as you said, even if you mandate an app, people will find a way around it, you leave it at home, etc. I do think the decentralized approach has been, at least from the privacy and security, from this perspective, this is the approach to pressure governments to take up to. And the pushback you'll get is, they will say, well, this, this gives health authorities a lot less data to work with, they won't know where outbreaks happen. They won't necessarily know when they happened. So there is a disadvantage to this. But at the same time, it just dramatically reduces the potential for function creep, and for abuse. And those are two criterions. And I think the third one is also, the UK experience also, keep watching out for other kinds of technology that are being used in the pandemic beyond the contact tracing apps. These can also be incredibly invasive. And maybe the last one is, sort of, always think about, the app needs to be designed in a way that people can use it, especially people who only have old phones. Who can't use the latest, who don't have, use the latest protocols. That's a big issue especially outside Europe, but also in Europe.

Greg Nojeim
I would just add a couple things real quickly. One is use of location information. It's very sensitive. And although there is usefulness to it now, you can know if the contact happened in a particular location, whether it's likely to have resulted in infection or not, it can be useful in helping determine that, but it's also potentially very invasive. On voluntariness, we have to go beyond the question of whether a government requires a person to download the app, an app can become effectively involuntary through the actions of others, such as employers who say, we only want a safe workforce. We want all of our employees to download these apps so that if one gets infected, everybody will get a notice. I could imagine employers going down that road and turning these voluntary apps into essentially involuntary, in a way that, for example, Google and Apple wouldn't be able to account for. Not only do we have to test for effectiveness, we also have to test for equity issues. Are the apps, or use of the apps, diverting contact tracing resources from the communities that are most impacted by COVID-19 to communities that have downloaded the app? Are we diverting the resources from the people most vulnerable to the people who are most tech savvy, I think we have to be careful. And we have to test for that kind of thing.

Carl Roberts
Great. There's a question that builds a little bit on what you just touched on, to some extent, Greg, from an anonymous attendee. And this person would like you all to address the issues related with contract tracing apps being used, not only in employment settings, like you'd mentioned, Greg, but also access to housing, access to the right to travel, and how that relates to privacy and rights. Is there some big problem there that's not just around employment, but more generally, is is there a real threat to privacy that's going to come from these apps serving this function?

Greg Nojeim
I'll add one quick thing from the US perspective, but then I want to hear from other folks. We don't have a good baseline privacy law that will prevent that kind of thing from happening. We would have to enact legislation, legislation has been proposed. It's not good enough. Hopefully some good legislation will pass. I doubt it. I'd like to hear though, what happens in countries that, for example, are under the GDPR. Could an employer require the act? Is there some bar to it? Or is it permitted, how will it work elsewhere?

Frederike Kaltheuner
So the advantage is that with a baseline privacy law, you end up being better protected. And you're not just better protected from sort of, there's the government, there's your employer, insurance companies. So there's an entire, there are different entities that have no business in knowing necessarily your health status, or knowing your health status could lead to disadvantages. In theory, the GDPR, for as much but offers protection, in practice it's a lot more complicated. And I think the fact that the UK government itself failed to comply with the GDPR, says a lot about the state of GDPR in Europe at the moment. There is a massive enforcement gap. Regulators are overwhelmed. Especially in sensitive areas when it comes to, for example, biometric data. Member States have making made use of derogations. So the laws differ from country to country. So I would say, the baseline is also, so it was interesting, in response to especially the employer question, different national data protection authorities have given contradictory advice at the beginning of the pandemic. And then, the European Data Protection Board clarified when their interpretation is. So I think there are a lot of there are a lot of concerns, though on average, you have more remedies, especially, you have data rights that you can enforce. So you can't just surveil, your employers, without safeguards or that consent.

Dev Lewis
I'll just add them from some shared experiences from Asia. I mean, of course, every country is different. But we've really seen the best examples of apps being used to regulate access. I talked about China already. India is doing it now. And now we've seen South Korea and Singapore to bring in the sort of safe access QR code functions, which is not necessarily just flashing an app for your health status. But again, in the form of, do you have? Can you scan? Can you register? in order to enter these premises? And so, I think, that the problem that Asia deals with, we've been dealing with this for years now, is that, you know, digital literacy is very low. A lot of the Internet users who are coming online are very new. They've been online for maybe a handful of years at best. And so, in general, you don't have a large awareness of what our digital rights might be, what kind of threats and violation might be, and, to make things worse, we don't have strong data protection regimes, because the GDPR is often looked at as an example, and you know, within civil society, we use that as a pillar towards guiding our discussions.

And, in India so far, we've seen an interesting push and pull. So Aarogya Setu came in as this app that the government, Modi himself said everyone must download the app. But then people pushed back, including the Supreme Court. And so you have this sort of mandatory not mandatory balance, where Greg mentioned, employers sort of encourage their employees to do it. Delivery companies, like platform companies, have all the delivery workers get the app. And, essentially you have this sort of, you have these quasi spaces, right. So you know, whether it's your company, whether it's your neighborhood, maybe your society will, you know, come to you, and sort of tell you to get this app. And so you have these like bubbles and spaces emerge, where it becomes mandatory, and then gradually that adoption increases and that's why India's been able to get it to about 100 million plus people using it. And given the fact that the majority of India's Internet users don't have access to smartphones, most have our feature phones, and so you really have a fairly high adoption so far. So I would say is that Asia really is the space to watch, where this clash between various invasive apps and systems, which then get deployed very fast, and you sort of get to see what's happening in real time.

Sabine Muscat
What do you think, Carl, do we have time for one more question, or should we wrap up on time because now it's 10 o'clock here?

Carl Roberts
If all the panelists agree, I think we can take one more question. Great. So I think something, something related that to that question that I think is also important and that we do need to consider comes from James Gezonowski, James from the US. Right now, Apple and Google is for public health authorities. Will Apple and Google open up the APIs for providers and payers, as the goal is to reduce spread in the community, and reduce impact to healthcare resources. I think, also more broadly, like how should we deal with organizations that do have a vested interest in knowing the spread, knowing if people have it, instead of these kind of groups like an employer where it does seem to be a clear breach of privacy, how should we go about data privacy around COVID in that field,

Greg Nojeim
One of the problems that they are trying to account for, Google and Apple, is false notices. You wouldn't want a person to be able to persecute other people by sending a false notice that the person had COVID-19, and that the people around them should self-quarantine, or go get tested, and be put into a very, you know, a state where they're very worried. So, the way that they are planning to do this, is that you'd have to have a health authority give you a code, or do the actual trigger of the notice. You do the trigger notice, but you couldn't do it without the Health Authority, and their participation. I think that's probably a good protection, as opposed to having others be able to trigger those notices without the participation of health authorities.

Sabine Muscat
Okay, if none of the other panelists want to weigh in on this, I will start concluding this session by thanking all the panelists for being with us here today. And really proud that we could make this happen really across three time zones. It's already very late for Dev. now, and very still in the morning here, so that's great. And I think what the debate showed has been that, yeah, we can really see a lot, we can learn a lot from this contact tracing app, and from the debate over it. And, I think, in the worst case, we

will see function creep all the way to bio-surveillance, as you have described. And it's important, therefore, to have these debates on how to protect privacy when using such unknown digital tools. But in the best case, we can say that, well, this has triggered, or renewed, the debate over privacy, all the way from India, where there has been incredible civil society interaction and actually pressure and pushback on this very intrusive Aarogya Setu app, and they had to backtrack on it. And so that's actually, I think, it's a good development in India. And also in Europe, it's a test case for GDPR. How how well will it work? And how do countries make sure that apps are GDPR compliant at the end, despite the extraordinary measures that are, of course, also, on a temporary level illegal And then the United States too, it has renewed the privacy debate, or it has illustrated the need for national legislation that has been shelved, of course. And, in the meantime, there are all these bills that are being introduced in Congress now, on like COVID-19 Privacy Act, the exposure notification Privacy Act, to make sure that these apps are not being abused. And so, definitely, it has increased awareness. And so probably that's the good part. And yeah, with that, I would also really love to thank the audience for joining us in large numbers. And I would like to thank the Center for Democracy and Technology for doing this jointly with us. And with that I wish you all a good evening or a nice day.

Dev Lewis
Thank you, everyone.