The University of Sydney | Sydney Ideas
Public talks program

TRANSCRIPT

Sydney Ideas podcast

COVIDSafe app: safe to use?

Tuesday 5 May, 2020

ANNA BURNS: [00:00:00]

Hello and welcome to the Sydney Ideas conversation.

I'm Anna Burns, the Public Programs Manager. Today we have a great selection of perspectives on this panel, *'COVIDSafe app: safe to use?*'.

As we start to chart a COVID-19 recovery course, there are a number of complex issues to consider.

Last week, the government announced and released the COVIDSafe app, designed to help us all to return to some sort of normal.

There've been a lot of discussions about the functionality and security of the app, and we'll consider those briefly today. But the other questions that the panel are going to consider are, how is this going to work? Can it actually work? Will that keep us safe? And also what are the risks to us all collectively and individually if we do download it or if we don't.

The purpose of this conversation is to give you access to expert insights and facts. We've got an extraordinary group of people who've joined us here today to help you evaluate the potential benefits, limitations, challenges, and other considerations.

Some of the best minds who are from the university here with you today are, Professor Robert Slonim, who's a behavioural economist from the School of Economics.

Dr Suranga Seneviratne, who is a cybersecurity expert from the School of Computer Science.

Associate Professor Jeanne Huang from the Sydney Law School will put this in context, both in an Australian legal framework and an international law framework.

And Associate Professor Adam Dunn is a specialist in public health informatics.

Thank you all for joining us today.

Bob, I'll start with you. What is the COVIDSafe app and why do we need it or not?

ROBERT SLONIM: [00:01:28]

So the COVIDSafe app is a contact tracing application that if somebody is to test positive for the virus, the idea is it's to add to the resources to be able to quickly identify others that they may have been in contact with, to let them know and to alert them as quickly as possible. They can go in and quickly get tested if that's the case or self-isolate. And so it's to help deter the spread of the virus.

I thought I would start with just a very quick slide here, just to say where we're at. As you've mentioned already, Anna, the app was introduced nine days ago and this is a graph of the number of people who downloaded the app since its inception. There was roughly about just under a million people who downloaded each of the first two days.

That has gone to about 500,000 over the next two days. And those numbers have been decreasing fairly steadily ever since and down to about 200,000 people that downloaded the app yesterday. These numbers are tracking, roughly speaking what Singapore, who has also had a very similar app to the one we're using here.

In Singapore's case, we've been able to see the longer term horizon and they plateaued, roughly speaking, at the same place that we're at currently right now. So we may be a little bit ahead of them, but there's a lot of worries signs.

My expertise is in behavioural economics and I think today in this discussion, one of the big comments I want to, I want to focus on, is that, I think we're asking the wrong question. And I think I actually, as a behavioral scientist, we know that the way we ask a question can heavily influence the way people think about the issues and respond.

I think the appropriate question here should be flipped. And it should be, you know, what are, what are the risks if we do not download this app?

This app is a tool that's going to help us stay safer. And the government and its presentation has been using for sort of euphemistically these ideas of, say, we're going to have a longer time in isolation. If we don't have these tracing abilities, we're going to have a longer time where we're going to have people in unemployment.

What that really translates to is a lot of harm to individuals lives longer. People are unemployed. It means that people are going to be going through more insecurity, income, insecurity, confidence in themselves. this is going to lead to a lot of stress in their lives. This is going to then translate into, as we've been seeing increases in people sort of concerned about their mental illness, mental wellbeing.

This is going to translate into greater inequality in society. This is being particularly felt by the people at the lower end of the income distribution that are being more hard hit by the stress that they're experiencing. These are really big social issues. And I think, the question we should be asking ourselves is, what are the risks to not downloading this app? And having this ability to do, have one more tool at our disposal to help us fight this virus and to keep it under control and not spread as much, not create a second wave.

ANNA BURNS: [00:04:21]

Excellent set up there, and we will be digging into a bunch of those questions. I might bring the rest of the panel in one by one just to sort of put them in a bit of context for you.

Suranga, the majority of discussion in the media so far has been from a security lens. From your perspective, thinking about security and its broader sense, like what are the big issues that you think should be considered here and the questions that we should be asking?

SURANGA SENEVIRATNE: [00:04:42]

Right. So I mean it's natural to ask all these security and privacy questions because whether this is, that these are governments or private companies, the security of the user data is not – our track record is not that good in terms of that. So people asking all these questions, whether this app is collecting something additional, are there any sort of back doors, and all these questions.

And also there are questions related to where this data is being stored, how long? Who has access to this data? I think all of them are very good questions. And people have the right to be concerned.

As of me, my expertise is in mobile security. I have been studying apps, especially in Google Play Store for five, six years. And I have been studying how apps collect data in the background it has been used for other purposes like advertisements and et cetera. I'm interested in answering any questions related to privacy and security.

ANNA BURNS: [00:05:53]

Jeanne, there's a really tricky conversation here from a legal perspective because there's a number of different frameworks that need to be covered simultaneously, both in Australia and in an international context around Amazon and data storage. Do you want to, just give us a quick overview of where things are and where the kind of question marks are?

JEANNE HUANG: [00:06:13]

So here I think we should predominantly focus on domestic law level of international law level.

So for domestic law, I think actually we are very pleased because today, privacy amendment bill has been introduced.

So we are waiting for our parliament to reconvene early next week to make the temporary legal framework, the biosecurity determination into the law. And currently the COVIDSafe app is based on the biosecurity determination, which is temporary; only last for three months, where it expires in June – so we need to make the into the law.

But I think it's very important, we should be mindful for three issues at a domestic level.

The first one is geographical imbalance because we are a larger country. We should be mindful of our Indigenous people and people in the rural and remote Australia, the internet part of Australia, the technology that work, may be very bad.

And the second issue is intergenerational equity, especially we need to provide more assistance to our elderly people, to help them to be better informed of the pros and cons of this app.

And the third issue is economic equality issues because here, actually, going back to the comment about the sunscreen issues. So actually you need to at least [be able] to afford a digital device but this may not be possible for all of us.

And regarding international level as just now, you mentioned about Amazon as a service provider. So there is an international agreement, the issues like whether we can include a provision between Australian government and United States government in terms of executive agreement under the US CLOUD Act.

And also another dimension is for transparence in our area, because nowadays we are discussing to open our border first to people traveled to and from New Zealand. So are there any possibility that we can harmonise or better facilitate the contact tracing transparence in our area.

ANNA BURNS: [00:08:40]

Thank you. We're quickly determining that the what seems like a very straightforward proposition – *to download or not to download?* – is actually a deceptively complicated.

Adam, this is a complex issue within a even more complex public health conversation. Going back to where we started, like, are we having the right conversation around this app?

ADAM DUNN: [00:08:58]

Thanks Anna, and hi everyone. So I'm Adam. Just as a bit of background, I'm the Head of discipline for Biomedical Informatics and Digital Health at the University of Sydney.

I spend a lot of time working on data driven methods in public health surveillance, and my team includes people who do social network analysis, study BLE, contact networks indoors. And I personally spend much of my time trying to understand how population health behaviours can be influenced by the information and misinformation that people are exposed to online.

So it is absolutely a complicated issue. My personal opinion is that one of the major issues that we have at the moment is around the communication and marketing of the app, not so much the app itself and the possible unintended consequences that that might have. So my opinion is that the app might lead to some small improvements in contact tracing efforts.

It'd certainly be valued by the people who do contact tracing to have access to more information that can help them do their jobs. But because we've been marketing it as a form of protection and tying it to the relaxation of social distancing policy, I think this is patronising and dangerous.

Ultimately, I think that the harm caused by giving people a false sense of security, will far outweigh any of the small benefits that might have, might have on contact tracing.

So in short, I think we should really be doing as much as we possibly can to support contact tracing, especially with things like digital tools, but we need to be really transparent and honest in the communication about that to avoid unintended consequences, like false sense of security, which could change people's behaviors.

ANNA BURNS: [00:10:32]

Right. So I want to dig into this question of security and going beyond data security, which you've all kind of raised already, and referring to the Prime Minister's description that the app is like "sunscreen". So there's a sense of protection here. For all of you, like, is that actually correct? Is it actually a protection or what are the false securities that we might be falling into? I will throw it to you, Adam, perhaps.

ADAM DUNN: [00:10:58]

I guess this is a really important one to think about. Let me start by saying we should first acknowledge the sort of the brilliant people that already work in public health practice, like especially the kind of hundreds of experts who already do contact tracing these are the people that we really need to be able to look after and mitigate outbreaks.

So, just earlier this afternoon, I spoke to Dr Emily Dido, who's a colleague of mine, and she worked in contact tracing for, for many years. And I asked her, 'Would you like this data? Would it help you?'

And she said, 'Yes, absolutely.'

It would be great to have additional data that can help them do their jobs. But I think we have to remember that this is a really complex task. These people who do contact tracing, and there are hundreds of those, hundreds of these people are in Australia, have substantial expertise in doing that.

They're kind of like hundreds of little Sherlock Holmes, running around trying to investigate what has happened and who's been in contact with everybody else. So then absolutely, they'd love these tools. But we have to think about this app in the broader context of its safety and its effectiveness.

And so when I'm talking about effectiveness, I'm not talking about efficacy. I'm talking about effectiveness, which is a measure of how well something will actually work in practice and for complex behavioural interventions like this, this kind of app that we're talking about, measuring effectiveness really means that we need to include things like long-term and unintended consequences.

So when I think about effectiveness for this app, I think about it in... let's think about it in a simple way. Let's say we get to this point where we have 40% of the people who've actually downloaded the app, and optimistically around half of those people are using that properly. If you're on an iPhone, that means that you've got it up. You know, you've got it in the foreground and you've got your phone unlocked. Then the chances are that if 40% of the people have downloaded the app, and half of those people are using it properly at all times, whenever they're anywhere, then the likelihood of registering contact between any two people is 4%.

That means that it one in 20 potential contacts will be captured by this app. And that's a very optimistic percentage at the moment with 20% uptake. And the fact that it's not, doesn't work on iPhones, that percentage is effectively closer to zero. So the other issue around that is that it gets, it gets actually much, much worse than that.

So last year actually, my team published in the *Journal of Biomedical Informatics*, a study that was looking at whether or not we could detect proximity and detect contacts between people using Bluetooth – this BLE technology – in controlled environments. And what we found was that everything matters. Obstacles matter, where your position, which room you're in, which direction you're holding the device – all of those things made a huge difference and it meant that the precision with which we can actually do this contact tracing is very poor, you know. And I think it's going to be much harder to do when everybody has a different phone and these, and the behavior of people indoors, outdoors; it just varies so much.

There was actually an article in the *Wall Street Journal* that interviewed one of the engineers who designed the concept for Bluetooth, and he said that, that the technology just wasn't designed to generate detailed reliable data about proximity between devices and that the accuracy is limited. So from my perspective, if we look at the efficacy, the effectiveness of whether or not this is going to work, it's going to produce a marginal positive benefit.

By providing the data that contact tracing people actually want, but in terms of winter and it's going to be effective, I would argue, not very much.

ANNA BURNS: [00:14:36]

So on that question of margins – Bob, where does this sit? Is it a distraction? Does it help?

ROBERT SLONIM: [00:14:43]

Yeah. Look, I think this is an incredibly important question, and I think if. If the effectiveness is as low as, you know, 100 cases we're testing, I think then we have very much worry as

Adam has just outlined very nicely about the concerns about being overconfident in the use of this and maybe taking undue risks. I actually have a slightly different take, which is, first of all, I think the marketing can be improved and the messaging can be done better.

I think of watching the news head of the US and people are listening to the medical experts and not the politicians. And I hope that people will listen to the experts here. And, you know, when Morrison says it's the safest sunscreen, you know, then we take that with a grain of salt properly, as I think we should to think it's going to be perfect.

A couple of things. First of all, both the Singapore government and the UK have indicated they believe the, the appropriate percentages of the population to be affected should be closer to 75 or 80%. And for the exactly the reasons that I think Adam was just starting to articulate, you know, if you think about 40% then first of all, you have to have your phones on and then these two people have to interact with each other. And this is why we need a much higher rate. I think that's really important.

I looked at Adam's paper, I was really kind of curious about this and the results in the paper to say that actually, even under the worst conditions that you've looked at, it actually was 52% successful at finding contacts.

So at least when the phones are within the distance, you're getting minimally 52%. And in some of your instances, they were actually as high as 80%. So it doesn't seem as miniscule of an effectiveness, just looking at that particular study.

More importantly, I think there are contexts in which this can be very effective. And I want to think just for a moment about our daily lives and where this is; where I think the other, the more standard interviewing people and asking them, 'where were you, who were you interacting with?'. You know, consider somebody that test positive who is just on, I'm on the trains or on a bus, or, you know, was at a cafe having a coffee with eight other guests around it. Which is a nice, stable environment. Everybody is sitting still together and it may not be effective, you know, and we want to think about it. For example, like we were talking about it in the opening remarks about in rural communities where people maybe know each other, they interact with all the same people. So that can work really well with other forms of tracing.

But in a city environment, in Sydney, Melbourne, Brisbane, Adelaide, and so forth – in our big dense populations where we're going to have a lot of incidental contact with people. Even on the train, just going to work. That type of context. This is where the device may be incredibly useful.

And it's also, there's a speed to this too. That is going to work very quickly. So I'm much more optimistic about the potential effectiveness, and I think that I'm more optimistic also about the marketing of this to be able to present it in a light that people understand. That you shouldn't just start walking out and going to the pubs and kind of going back to doing no other forums of the social distancing.

ANNA BURNS: [00:17:42]

I'm going to come back to the questions of inequality in a minute. But, Suranga there's a couple of questions that have come through here about how it actually works.

One of the questions is around, that you can use a pseudonym to sign up so that while you're, you know, you're being tracked with your phone number and, you know, there's, there's information about where you're going, but they, you know, tying it to yourself as a bit, there's a few sort of steps there of, of anonymity and a privacy. There's also a number of other questions here about how does it actually work?

SURANGA SENEVIRATNE: [00:18:09]

Oh, right. That probably, I will start with the contact racing part of the, and the effectiveness, which Adam and Bob already sort of discussed. I think, essentially the idea is that when, when two points in proximity, one transmits the Bluetooth signal and the other one captures.

So, and the app itself use the signal strength of the Bluetooth signal as an indication of proximity. Which is questionable, because it is not designed for that purpose, as Adam mentioned. And also the signal strength depends on various other factors. So yes, it might capture a scenario where you are in a praying with an unknown person who was in the proximity. It might help in those scenarios. But it also creates lots of, it might create lots of false positives.

And in some cases, many important contacts it might miss because there was no proper signal strength. The contact duration was not enough. So, I mean, it is a thing you could try in your tool set of fighting against this. But considering it tasks, the solution, I think the message needs to be sort of, you know, clear in that sense.

So the second part of the question was, how the data is stored, right? Yeah. So I think, so one thing we have to be clear is data is being uploaded to the cloud only if you have been identified as positive. Then the health authorities will request to upload the data. Before that, there is nothing uploaded apart from your phone number and you can give your real name or the pseudonym.

So in that sense, I would say, you know, if you compare other applications in some other countries like China or South Korea, which actually collect bit more information than, for example, it might actually collect absolute location in the form of GPS.

So in terms of losing your identity and sort of, you know, whether this data can be used for some other purpose.

I think the risks are quite low, low because just the fact that you are uploading minimum information only if it is required. That's my take on that in terms of data security.

ANNA BURNS: [00:20:41]

Right. And to extend on that, there's a question here from Kevin who's asked about, 'At the end of the life cycle, what happens when the situation's over? Where does that data go? ' And perhaps there's also a question here for Jeanne about the international kind of side here with America and Amazon.

SURANGA SENEVIRATNE: [00:20:57]

I think probably it's Jeanne, can answer the questions better, but I think I want to upload the data the duration is 21 days, if I'm not mistaken. And after that, the data is being deleted, but probably I think Jeanne can explain better.

JEANNE HUANG: [00:21:13]

Yes. So I think that people have a lot of concerns, whether people outside of Australia may have access to our data.

I think there are three levels of questions.

The first level concerning Amazon is the data. That has already uploaded to the national data store. Because Amazon is a contractor to store the data, amazon is a US company, so in United States, and there is a law called the CLOUD Act, which require all USA data and telecommunication companies must provide that data information they stored inside or outside of the United States, upon the warrant.

In principle, the CLOUD Act also provide companies like Amazon, they actually take challenge the warrant. For example, they can file a motion to a court to modify or coach the warrant. So for the United States court, there are three arguments can be made.

The first one is the national interest of Australia. And the second one is, releasing those data, we are violating Australian law. So for example, biosecurity determination.

And the third issue is that data, the personal information, in this data space, it's not US citizens or US-permanent green card holder. Because the CLOUD Act many apply to the US citizens or the permanent green card holder. So actually three arguments can be made.

[00:23:11] But I understand the concern is, here we talking about that the US law. It is the US court to interpret the US law. So as I suggested at the beginning, our government, that actually seems [since] last October has been negotiating on an executive agreement with United States under the CLOUD Act.

So we need to impose an obligation on United States under international law, 'I need executive agreement to include a provision'. For example, in whatever situation the United States government and its court shall not allow disclosure the data from that database.

And the second level, actually, Suranga just now mentioned, before you upload the data flow, your mobile phone to the national data store, all the information actually is inside of your mobile phone. So in case that, your mobile phone has been hacked, so actually the biosecurity determination is not applicable to the security issues of the data stored on your own mobile phone. So here you need to look at the other law, for example, Privacy Act.

But please be mindful the protection in terms of disclosure of information under the Privacy Act is lower compared with the biosecurity determination.

And the third level is, even under the biosecurity determination in some circumstances, the data can be disclosed to people outside of Australia. That determination make it very clear this is only for the purpose of contact tracing. So actually there are three levels of the questions regarding whether that data can be released to person outside of Australia.

ANNA BURNS: [00:25:17]

There's an odd tension going on here that we're all really anxious about, or a lot of people are anxious about this app and the relationship with Amazon and Amazon's legal standing in America, but we all have Google maps. Many of us have Facebook, TikTok or WhatsApp, any number of other apps that are held under jurisdictions outside of Australia. Why the concern about this particular app? Robert, what do you reckon is going on here?

ROBERT SLONIM: [00:25:44]

I think that's, that is spot on. A very important question and it's not clear.

It's not clear that to me, that I've, you know, in reading several hundred articles about this now can understand why this technology has particularly received the scrutiny other than that it's coming from the government. It's, first of all, we should keep in mind it's volunteer. They're not saying your mandate, you have to do this.

But I think whenever there is something that comes from the government, it appears to be that it gets a higher level of scrutiny. People are concerned about, “well, what's the government really up to?”

I actually feel in one respect, this might be about as safe a thing as out there right now as a technology device because the government has put this out there. The government has said, this is going to be private, this is going to be secure. There, you know, we have a Prime Minister putting himself on the line, you know, saying how, how this is going to work. And I, and I think if there, you know, if this fails, if there are privacy breaches, there are a lot of people that are staking their professions and their names on this right now.

They're saying that, that the certain actions is, Adam said at the very beginning, if we reach the 40% threshold, there are certain actions, you know, we can start relaxing a little bit. You know, it doesn't mean the open everything up, but maybe we move towards, you know, certain things can open up and you can start moving 20% capacity into certain facilities, or something of that nature.

And I think actually in some ways it's interesting to me that, I think we should trust the government here and let's put them on the spot. Let's, you know, let them deliver. They've put themselves out there as, as saying, this is safe. This is secure.

You know, the website that we developed that you saw that graph from. We've asked, you know, hundreds of people that have looked at this material. They've actually told us they think it's safe also. They've endorsed this app, you know, from all walks of life, from tech sectors, security sectors, cyber folks. And I think one of the points that I think is really important to you is to find out, you know, I think, you know, at some level we should trust the government.

You know, we often say we should never trust them on anything, but here's a chance to help fight it. You know, just like we stood up when we had bushfires and just like, we stood up during the drought and people went out and were helping. Here is another opportunity. We've been kind of bombarded with these in the last year, but this is really important and this is another place where we could spend five minutes to download an app and give a little bit of trust. And if this can help, it's great.

ANNA BURNS: [00:28:12]

So jumping off from the trusting the government thing, and going back to the function of the app, Adam, there's a question here from Simon saying, 'Is this actually even a contact tracing app? Google and Apple changed the name of their approach to exposure notification to better reflect his actual use and purpose.'

ADAM DUNN: [00:28:28]

Yeah. So let me quickly take the opportunity to jump back a little bit and talk a little bit about the security and data privacy.

Look, the government is being seen to be doing as much as they possibly can. To make sure that people are, are very well protected. And that includes not keeping too much data, or keeping data where it's less risky – all kinds of legal protections that they might try and add to make sure that malicious use of these data are avoided.

But it's not really a surprise to imagine that, that Australians are a little bit wary of government accessing their data, with the number of times that, that we've seen problematic failures in the past and people have been burnt.

I mean, it was just on the – what was that? – the 3rd of May, that another data breach was exactly was identified and they've exposed personal details about 70,000 people.

Earlier, I think it was even earlier this year, law enforcement initially denied using the Clearview facial recognition software. But the fact that they were using it was then leaked and then they were forced to admit it afterwards. So it's not really a surprise that people have been focused on privacy and security issues in relation to their data.

However, the government is doing quite a good job as far as I'm concerned in trying to allay those fears, and to try and make sure that the use of the app itself is safe.

Then moving on to the question that you had around, is this really a contact tracing app or is it exposure notification? I think that's exactly right. I mean, this is a tool that would add to the armament of contact tracing. The question really is how much does it add to the armament of contact tracing? And I think we should absolutely be around to support people who do this very important work as much as we possibly can, and give them all the tools that they can use to make their job easier.

But the challenge of course, is that it might be a lot of effort and a lot of work for not much benefit. And I think that's maybe one of the reasons why it's going to be a challenge. And so I think it's probably one important question to ask is it doesn't make sense for people in the government and influential people to try and convince up to 70, 80, 90% of the population who have smartphones to download the app. And of course it's in their best interests.

But I think one of the major problems we have is that the people who are trying to communicate this are treating Australians like they're stupid by telling us that, that this app is like “sunscreen”, it seems ridiculous to me.

If we want to use this analogy, you want to stretch this analogy out. It's not sunscreen. It's the world's worst UV indicator, and it only tells you that you've been in the sun maybe a week after. If, and it might get it wrong.

And so I think that that's the problem here is, is not so much whether or not people download the app and whether or not it actually helps people with contact tracing. It's the fact that the communication may lead to a false sense of security and that might lead people to go out and to abandon the precautions that they've been taking over the last couple of months to avoid risky behaviors: standing too close to people in line at the supermarket. Not wearing masks. Having parties. Going and watching people kick balls around on a sports field. And getting drunk with their friends. I mean, those are the kinds of things that, that we would love people to be able to do for mental health and probably for the economy as well.

But telling people that an app is going to be able to protect them from that is a mistake.

ANNA BURNS: [00:32:04]

So what are the impacts of false security, but also the, you know, the impact of potential false alarms?

Like you've, you've all alluded to the problems here that the data might not be quite right or, they might be false alarms. What does that actually mean from a... actually, from all of your perspective – if you're mis-identified or that data is stored somewhere else, what does that mean?

ROBERT SLONIM: [00:32:29]

So I think one of the very first, and so I'm very empathetic to the concerns that, that Adam's raising about the wrong messaging here. And I think that that needs to be tampered down. I think we do need to be realistic and tell people the truth about what this is, what it can do.

And what its limits are. And, I think if, if the message out there is, download this app and I can, you know, go to a pub and high five everybody and drink beer with people and get really close to them ... You know, go play sports and we'll sweat on each other again and so forth like that and think that this is gonna protect us – then we've got a real problem and we need to be, we need to reinforce that.

[What this is, is at the margins. You can understand, I think a little bit why they're trying to sell it. They're trying to sell hard [to] people to convince them to download the app. But if it's going to come at the cost of over-exaggerating, what it can do that that's an enormous risk.

So I think one of the things we can do here as experts, what I hope the message is back to the government. To the ministers to the Prime Minister, is to make sure you're messaging this and treating us like we are intelligent and can understand this. So I think that's an enormously important first thing that needs to be done.

In terms of the other concerns, such as a false positive, there's two aspects to it. One of which is people's people are going to get this information and this is going to cause the, what we'd ideally like is for them to isolate and get themselves tested right away. And if it's a false positive, there's sort of the, there's the direct cost, which is to them of having to go and address this and getting themselves tested.

I think that's right. Might be an actual, very small cost. And actually even could even have some benefits in the sense that it's just more testing being done.

But I think the real cost here that we have to worry about is, is it causes undue stress. And again, that's again, part of the messaging that I think needs to be really clear.

You've been identified, there's been a contact, there's been an indication here that you may have been in the proximity of somebody who is, who has had this; at this point, we don't know for sure, and we need to be honest about that also. Just like any other medical diagnosis that we were given, usually the first time you do it, you're told to get a second opinion. You should follow up on this. And I think that needs to be very clearly communicated here too.

I guess I'm a strong believer in people are quite intelligent and I think we can communicate this honestly and get the benefits of it, and we should be able to, at the same time, simultaneously minimize the risks that I think we can address, if we're just careful about this.

ANNA BURNS: [00:35:02]

So, Jeanne, are there any sort of legal implications here? If there's, if the data is a bit unstable and people are being falsely kind of identified, are there any considerations there that need to be worked through?

JEANNE HUANG: [00:35:14]

So I think actually there are two issues. The first issue, going back to Adam, talking about the miscommunication. Actually I agree. The app it works like a sunscreen is a misrepresentation.

Regarding the communication, actually I understand why people have concern that the app may become a beginning, like a digital surveillance. Like in China. Because, I specialise in Chinese law.

And I think that in terms of the communication, we should distinguish these apps and it's related the legal framework from the Chinese app. China also implemented, actually it's compulsory – strictly compulsory – the health code app for people to use. So the relevant, the legal framework and relevant apps are very different.

From my expertise, I don't think that there is a possibility, based on the current legislation, overall our code and our legislature system, these apps can become a beginning of digital surveillance? I don't think so. So this is the first part on my observation.

And the second part of, regarding the false identification, false information. So the biosecurity determination, that's not a justice issue. So the biosecurity determination as well as the bill actually only focus on the connection, the connecting information, use of information and disclosure of the information. So I think the false information is very important. So maybe better to adjust the from both the Commonwealth Law level and the state and territory law level.

So regarding the Commonwealth law level, so actually we have other legal framework may be invoked. For example, our Privacy Act. For example, our consumer law.

In terms of state and territory, so actually, you know, the biosecurity determination is a federal law. So in each state and territory, there is a state and local law determining how the health authority, the local health authority, shall use the data for contact tracing.

So there may be some gap between, you know, the federal law, the Commonwealth law, and the state and territory goal. A more important that is to ensure that consistency at each state territory, they can detect, they can identify the false information. And also I think they should be ready with the penalty for people, you know, purposefully to get the information law.

ANNA BURNS: [00:38:05]

Suranga we're talking about sort of issues of false information, but also there's a question that's come through – a question from John about the risk of the data being used for, so things other than COVID-19 contact tracing as well.

SURANGA SENEVIRATNE: [00:38:20]

Right. So I'm in, let me just, for the misinformation and message being clear part, I think that one thing that might for like, whether we can see some numbers now they're past being there for some time - can we get some information on success stories? Like, you know, so we identified this, this many people were informed, like, you know, whether there are some information on the success stories. I tried to find it in Singapore. It doesn't seem like there is not much information, but that is something that will really help, you know, encourage people to download the application.

Then it seems that this new legislation does not allow that. Probably, again, I would get Jeanne's opinion on that.

And also we have to, I mean, if we had a thing that the app doesn't, so there are storage constraints. If you are not get notified, like if you are not getting tested positive, that data doesn't really, doesn't go beyond your mobile phone, right. And if you think that that is a risk with the data being there and being hacked, I think that risk is therefore in your few other apps like Facebook, email or any other, right.

So in that sense, I think it's partial data. And the legislation doesn't seem to allow anybody else apart from the health authorities accessing that data. And also it is being stored only for limited amount of time. So I would think the risks are quite low in that sense.

JEANNE HUANG: [00:39:56]

So going to back to the question. So actually, based on the biosecurity determination the data can be used for purpose more than contact tracing. The determination provided very clearly there are three possibility to use the data.

Predominantly it's for contact tracing, everybody agree. And the second possibility is for investigation and prosecution of offenses. And the third possibility is for the identify the data for statistical purposes.

But as I understand, the question actually is whether the data can be used for law enforcement other than investigation, offenses, investigation and prosecution of offenses relating to COVID-19. So, for example, immigration officers – so whether they can use this data. So the biosecurity determination, clearly saying, “no”. No. Okay.

So actually here we should distinguish it, this app from the Google map or Facebook app, et cetera. Because Facebook and Google app, they are subject to Privacy Act and the Privacy Act and other legal framework actually allow the law enforcement agency, for example, policemen, immigration, border control, et cetera. They use those stakes.

But for biosecurity determination, it very clearly provide: the app, the COVIDSafe app, the data connected is not allowed for other purposes, go beyond the three just now at this stage.

ANNA BURNS: [00:41:42]

Two big things. I want to just really quickly touch on: the question of equality and inequality that the app's not affordable for everyone. What about people in indigenous communities? What about people, older members of our community?

And what happens if we don't get enough uptake?

ROBERT SLONIM: [00:41:59]

I think there's two questions there. So there, there is no doubt that, you know, the direct benefit, you know, it is clear to the person who has the app if they're going to be identified, if they're told that there's a contact rates, cause they can be able to react quicker than somebody that doesn't.

But the value is beyond that cause it's really to everybody. Because the idea is we're trying to suppress, you know, we've heard this term, you know, to, we want to flatten the curve, so to speak. Right? We've heard that so often here. The point is if we can catch a case, it's not just the person that we caught, but it's all the people they spread it to and all the people that they then spread it to intern.

So it's kind of the equivalent of thinking about why we take a vaccine when I take a vaccine. It's just not myself that I'm protecting. But the fact that now I'm no longer susceptible to whatever the virus is, is out there. I can't spread it to anybody else. And so it's a public good when somebody downloads this app and it doesn't just help them, it helps everybody in society because it's reducing the risk across it.

It's clear that, you know, at a firsthand, people that have the technology will get the most direct benefit immediately. But it's really a societal, it's really the entire Australian, no community that benefits from this. If it's maybe a secondhand effect that we're flattening the curve button, the curve helps everybody to the point of the inequality that arises.

If we don't download this app, we're experiencing that every day right now. I could give you many, many examples, but let me just give you one. Take the space of education. If we’re thinking about that some people have access to technology and other people don't, is the parallel here. You know, we live on the North Shore of Sydney and I, for the most part, from my neighbors, friends, families and everything else, I've seen very little sort of loss in education that's happened. There might've been a school closing for a day or two as they moved to Zoom technology like we're doing right now. Most kids are being educated. In fact, lots of afterschool activities are still going, music lessons and so forth. And you know, yeah, there's a few things. So some kids are not being able to do sports activities. You know, there's some activities that have that that can't be done. Many people are doing their yoga lessons or gym lessons still through technology.

And so those who have technology, I think are very much dramatically less being affected. But to the people that we're worried about that don't have smartphones and don't have technology. They're also being adversely affected. The longer we stay closed, they're going to be less likely to have access to schools.

They're going to be less likely to be able to benefit from education during this period. If they can't go to school and they have, you know, intermittent email (I'm sorry), intermittent internet access or communications and being able to get that same level education and that that's happening every day right now, as in sort of the spreading the inequality.

And so I think that. We could go through countless examples of this inequality that's occurring as we stay, and the quicker we can get people back into the classroom. For that example, I was just saying, the more we can suppress this. State governments have done a really great job. Victoria, New South Wales – I've been paying attention to in terms of trying to get every kid, everybody that doesn't have technology, but it's not perfect and it's clearly not, you know, it hasn't happened quickly and there's going to be holes in that and that inequality. I think it's going to be really, you know, a major issue that we're going to have to face.

ADAM DUNN: [00:45:22]

So can I jump in then? Look, inequality is one of the major important things that we need to think about through this entire pandemic. t's absolutely true that people who are from marginalized and vulnerable communities are going to be to be people who are most affected by the pandemic.

These are the people who are more likely to lose their jobs, more likely to suffer from mental health issues and more likely to be affected by, the kinds of things that other people who are in less marginalised and vulnerable communities are not effected by. I think that that's pretty clear, but there's also this false link here.

And the false link is that we are attempting to try and tie the downloading of this app to the reopening of schools of businesses and borders. And that's not just not actually true. I mean, at the end of the day, regardless of whether or not this app exists, at some point, we're going to need to bring down a number of community acquired cases to the point where we can effectively do contact tracing for every new case that appears. And, that is independent of the presence of the absence of this app.

It's true that the app is potentially going to support and help to do contact tracing, but at the end of the day, that contact tracing is really the people. And the tools that they already have at their disposal that we really need to focus on; if it was up to me, I'd spent all of the time and energy on training and supporting and looking after these contact tracing people so that they can do their jobs effectively.

And I wouldn't muddy the waters by trying to convince people or essentially hold their social lives hostage based on how many people have downloaded the app.

ANNA BURNS: [00:47:08]

Suranga, have you got anything else to, to add in to the mix before we wrap up for the afternoon?

SURANGA SENEVIRATNE: [00:47:15]

I think I fully agree with what Adam said. Like, I mean, we, at least at this stage, we can't directly correlate the application downloads, the adaption of this application, to how soon we can open up the situation, et cetera.

I mean, as Adam pointed, the accuracy of the contact raises, how effective it is. So, I mean, I think that message probably needs to be clear. It's at least, I'm not that convinced that it is directly related to reopening the shut-out.

ANNA BURNS: [00:47:51]

And Jeanne, from your perspective, what do you think of the key things that we need to, as individuals, keep in mind?

JEANNE HUANG: [00:47:58]

I think, first, the app is a good idea. But the it cannot replace other contact tracing measures as Adam described, the human being. I think that's very important.

And the second is the equity and the equality issue that you mentioned. It's extremely important. It is not only for the app, but also, if we look at, slow out the pandemic, that might just let our government to take for example, the lockdown, the social distancing. So as a professor actually, my job, I can do all my job at home. But imagine that if my students, and they work in the cafe and their job, but actually they lose their job.

So you'll see the very imbalanced impact of the measures in the pandemic to different, you know, status of the person. So actually my message will be: after pandemic, we need to take a holistic approach to reveal the measures that, you know, the urgency [of] measures that will [be] taken, we should have a holistic approach to address the equity and inequality issues in society.

Thank you.

ANNA BURNS: [00:49:14]

A good call to arms and a few sort of small things to tackle in the coming days and weeks. Thank you all for your time this afternoon.

ANNA BURNS (PODCAST OUTRO): [00:49:22]

Thanks for listening to the Sydney Ideas podcast.

For more information, head to sydney.edu.edu/ sydney-ideas; it's where you'll find the transcript for this podcast and our contact details if you'd like to get in touch with a question or feedback.

If you haven't already, subscribe to the podcast so you never miss a new episode. Search for *Sydney Ideas* on Apple Podcasts or SoundCloud.

Finally, we want to acknowledge that this podcast was made in Sydney, which sits in the land of the Gadigal people of the Eora nation. It is upon their ancestral lands at the University of Sydney is built.