Safe to Trace: Mitigating the Cybersecurity Threats of Contact Tracing

June 9 2020

Franca Palazzo
And citizens for a affordable, accessible, safe and open Internet. More important than ever, I would say during these crazy times. If you are not already a member and would like to support our organization and the work that we do, you can go to Internet society.ca and become a member there. So I want to start by thanking my co chair, Jeremy Dapow. And all of the panelists that have agreed to share their time and expertise today. Special thank you to Lena Trudeau who is our moderator and will be she helped quite a bit in the organizing of the panel. I'd also like to thank jack Johnson and Alessia mazzoni who helped with all the social media and technical work that we were doing. So I'd like to hand it off to Jeremy Dapow, who will tell you a bit more about the project, the IoT project that this kind of is a tangent of and what we're going to be doing going forward.

Jeremy Dapow
Thanks, Franca, and Welcome, everybody. And thanks to our panelists and our funding partners and partners and, and we're excited to have you this discussion today. This, this webinar has been born out of an initiative that started quite some time ago with the Internet Society on mitigating IoT, particularly consumer IoT cyber security threats. And we initially had a plan to do some in person forums, and we launched that in February 20. And we had a great discussion, contextualizing mitigating consumer IoT, cyber security. Of course, the world changed then and since then. And so what we've done is, is we've transitioned this project, as everybody is into online forums. And we're very pleased by that because it's easy for people to have access to. And it's also a little bit easier to get the very intelligent and informed speakers and panelists, so we have with us today. So, from that initiative, we've decided to transition to these more brief web webinars as opposed to full day sessions. And we're going to be covering a number of topics related to IoT security over the coming months, and this is an ongoing project that we are continuing and of course, right now we are in unprecedented time that has put the fast forward on technology adoption. And with the fast forward we have great benefits, such as perhaps some benefits with contract tracing. But we also have new vulnerabilities with with the increased solutions and different platforms. And so, we're excited to, to continue to have these discussions and so today we're going to talk about cybersecurity and safe to trace discussion on contract tracing applications and safety. And we've got a wonderful group of people with us today. And you should have the opportunity to ask questions in the q&a box at the bottom of your screen if you're using a computer, maybe a little bit different on the application. And we also invite this project is something that we're work in it we're

continuing to, to build out. The first forum's report was released and it is on the Internet Society Canada chapter's website. And if you would like to get involved and help fund this initiative, we certainly invite that and we invite participation as well. So thank you very much. And, Lena, thank you for, for agreeing to moderate this session. And Lena and I have been good friends for quite some time and I've someone I admire very much, President and CEO of U Group, someone that has advised the Canadian federal government with the Digital Public Service, also has advised and United States and in where that kind of initiative originated and has served with Amazon in the past. And a great leader. And thank you Lena, for for, for agreeing to do this. So over to you.

Franca Palazzo
I'm just gonna jump in Lena before you start, one thing I forgot to mention was if you'd like to tweet today hashtag #safetotrace and @Internetsociety.ca that would be great. Lena? Another part of her bio, one of my best friends.

Lena Trudeau
I love doing events with you all. So I'm a member of the Internet Society, the Canada chapter of the Internet Society and in that role, I have the opportunity to work on really meaningful projects and initiatives that have implications for the lives of all Canadians, which is a really great honor and I'm so pleased to do it. And I know that Franca mentioned earlier that if you if you're interested in these issues, you might want to look at InternetSociety.ca. And consider membership. It's very low cost. It's a grassroots effort. And it's really aimed at protecting the freedom of the internet and access to important technologies with consideration of critical risks on behalf of all Canadians. So that Franca, thank you. And Jeremy, thank you. Thank you both for all of your hard work in setting up this event. I can't think of a more timely issue right now than the one of contact tracing. And so if we do our job here today, we're going to make sure we address a lot of different aspects of the question around contact tracing and security, IoT, cybersecurity, so many aspects to it, but we really want to know, you know, a little more in depth, what is it and how does it work and what are the different models for deploying it? Is there good data behind its effectiveness? Because it holds the promise of being able to help us reopen more quickly, and reach economic recovery more quickly, by allowing people who've been tested and who were infected, to trace across their networks, the contacts that they may have come in touch with, and allow those folks to quarantine helping improve safety for all of us. Right. So the promise is a really great one. But there's there are questions, first of all about what it is and how to deploy it. And then there are a number of questions that we want to consider today in our discussion around how do we ensure that the right governance models data privacy and security mechanisms are put in place to ensure that as we use these technologies, we're protecting the rights of everyone to the extent that we possibly can. So without further ado, I'm going to introduce our panelists one by one. I'm not going to introduce everybody at the beginning, if that's okay, I'm going to go first to Chris Parsons, who's a senior research Associate at the Monk School, the Monk School Citizen Lab, which I just think, is the coolest name ever the notion of a lab and experimentation and research around things that are directly focused on the citizen at the University of Toronto, and Chris, you've been doing public policy work on contact tracing specifically. So maybe I could turn it over to you. And you could help with setting the tone for us this morning.

Chris Parsons
Yeah, so thank you very much, Lena, for that. And I just want to thank ISOC, and Jeremy. And everyone really has been involved in putting this together. I'm all too aware of how challenging and how difficult it is. And I know that Franca has done a huge amount of lifting. So thank you so much for putting this together in these challenging times. So, you know, we've been asked to keep our comments very brief, which I promise I will do. I just want to touch on a few pieces. So the first is, I think it's important to recognize there's a promise in contact tracing, but the question of accuracy is important. I'm just gonna touch on that really quickly. And I'm going to talk about trust and why trust is so important to any meaningful cybersecurity solution. So to begin with around efficacy, I'm sure we're going to discuss through this, this panel, there are questions about how useful these tools are. There's contact tracing. And this is a process whereby often Public Health Officers will know oh, this is where Chris has been using people he's been around, and they can do notification. And there's exposure notification, that tends to be a situation where it's more privacy protective. And so rather than that information being shared directly with public health, the people who I've been proximate to will get some sort of a notification if they had installed an application and had a contemporary version of their their operating system on their phone. And I'm sure someone else on this panel will talk in more depth about that. But there are questions about how useful this is. This is a very new technology. The promise is we use this now because COVID spreads quite quickly. And this might be a way of informing people that they are indeed potentially infected. We don't know how well that works. We know in Singapore and Korea, that really we don't have a particularly high uptake of these applications. And we don't yet have a strong data showcasing that has been essential in addressing or mitigating the spread of COVID. In those jurisdictions. At the same time that we're talking about contact tracing, there's a large number of other things that we might want to use our ICT skills for that I just want to raise. We also may want to think about more broadly, you know, this conversation but for the efficacy of how ICT can work So as an example, for travelers when they arrive, do we have an application that helps and guides them through that process? Do we have diagnostic information that's, that's provided and is widely available? Do we have applications for quarantine to ensure that people are honoring the quarantine guarantees? And are we building systems that improve the epidemiology process. So something actually helps a contact tracers themselves, you know, from South Korea, they went from taking a day to pull all that data together and contact someone 10 minutes. So there's different ways that we can envision ICT is really improving the ability to respond to COVID. Now, in all of these cases, of course, security is going to be paramount. I want to talk about two kinds of security, technical security. And what I think is actually more important, which is social security or social trust that leads to security in terms of technical security, within the Five Eyes, so that's Canada, the US, UK, Australia, New Zealand, but not restricted to them. There's an ongoing debate about whether or not strong encryption should be provided to customers and consumers. This is the kind of encryption that is unbreakable by state adversaries or anyone else. Now, why does that matter? Usually this is a law enforcement discussion. It matters because individuals who are using tracing apps or exposure applications, probably want to know that their data is secure. And part of that means they need to know that the way their data is secured, is actually secure. And that means that governments have to be very clear in their messaging, if they're not going to modify more broadly how they're going to talk about the availability of encryption, they least need to make it very clear with press these health applications, that they are indeed, insisting in demanding the strongest encryption is available to secure that data at rest and in transit. But beyond that, we know software will have bugs. This is just the law of software. And quite often groups such as

the citizen lab find vulnerabilities in code, there needs to be a way for researchers who who are trying to do good work to report those vulnerabilities to software developers without the fear of litigation. And that might seem like a sort of a silly thing to raise at this time. But I have any number of friends that they don't report vulnerabilities they find every day, because they've been threatened with litigation time and time and time and time and time again. So do companies that are building the actual contact tracing or exposure notification applications. Do they have a vulnerability disclosure program they have, we have been taking that information without threat of legal consequence. So those are two technical things I would want. But neither of those actually are all that important. In the greater scheme of things they matter. I don't want to put them aside. But none of that matters unless the social trust is there.

Chris Parsons
And so this means that before we even deploy these applications, there needs to be really robust and meaningful engagement with stakeholders who aren't just in the technology community. That means going into communities that are historically targeted by police, Public Health Officers and so forth, or have histories of inappropriate over policing, or over monitoring by public health authorities. Because we know that as an example, law enforcement routinely demand access to people's phones, in particular targeting black men and women. Well in a contact tracing app environment, you can picture an officer going up, someone is perceived to be coughing or having a symptom and saying, Oh, I want to see your status because I think you might be sick. And then as soon as that phone is unlocked, as soon as the status is revealed, there's a fishing expedition on the phone. So we need to ensure that the persons who are most discriminated against, who often are disempowered in our societies are the ones who are deeply involved in the discussion. Is it going to be the case that these tracing outs are going to just be used for notification? Or are they going to be used by employers, you have to show your status come to work, and you have to come to work. Because if you don't, you can't be paid. There's going to be a situation where you have to show your status to get on public transit. And if you don't show it, no transit, which may mean you don't go to work, do you have to have a demonstration of status to go to a park, and so on, and so on, and so on. So that means that we have to have inclusive discussions. We have to bring stakeholders and it can't just be people around the table and talk and then government does what they want. They actually have to consent and agree wholeheartedly. Now why does that matter? Why is this a security issue seems like a social policy issue more than anything else, perhaps. It's because if we don't develop social policies, political policies that are appropriate, people will be incentivized to cheat the applications. And when individuals have their literally their lives on the line, not from COVID, or from their ability to go to work, pick up groceries, things of that nature, they will be motivated to cheat. And you can be sure that there will be populations that spawn up to help them do that. And these will not be bad people. These will be people who can put in a bad situation by bad policy. And so I think it's really important to get the technical aspects of COVID tracing or exposure applications, right, we need to figure out the correct governance of the data, how will it be handled, how it will be deleted, but we really need to figure out that social policy because if we don't figure that out, if we just bring these applications out, we're condemning them to failure and that's probably not what we want to do after we have invested hundreds of thousands of hours in developing the applications, deploying the applications, and hoping that these applications can actually help. Thank you.

Lena Trudeau
Chris, thank you so much, so many aspects of this very complex issue to think through. But I particularly love your concept about the need for good policy in order to ensure the right level of inclusion and engagement. So that ultimately, people aren't subverting the technology and therefore its effectiveness. Thank you very much for those comments. I'm going to go to Mary Jane Deichmann next and Mary Jane is founder and partner at Inc data law. And she also has a long standing healthcare practice. And so that intersection of health and data and policy and, and, and law, I think is one that's really useful for us to consider in the context of this conversation. So Mary Jane, what are your thoughts on contact tracing the need for it and the implications of it from your perspective?

Mary Jane Dykeman
Thanks, Lena, and thanks everyone for the invitation today. It's such an important issue. This is the one that is literally the crossroads, I would say. So COVID, being a health lawyer, long standing health lawyer, and having had the opportunity to work on the development of Ontario's health privacy legislation, and then also working in data. It is the marriage is what do we do with the data? How do we invite and I say invite quite specifically, people to contribute, because we'll have a discussion of whether this is something that will be voluntary. How effective will that be? Or ultimately, could it be imposed? So just to take it back to basics from a legal framework point of view? We have public health legislation federally and in different provinces and territories. I look to our health protection Promotion Act, we always talk about what does it mean in terms of privacy. But we have to keep in mind that public health legislation is a strong tool. And it essentially boils down to there are powers that exists that can set some of those things aside, maybe not entirely. and public health legislation is typically meant to be the least intrusive measure. It is meant to be time limited in its application. And as we wear our hats of protectors of data, we want to see that data is not going to be used for a purpose other than the one that we've told people that Chris led right off the top with the comments on trust. So I would say that trust and data governance are going to be the real imperative. And it's not to say that this will not happen, because the technology is different today, even when I think back to being in House counsel to a hospital during SARS, and in the trust factor, but we were not as advanced in the technology. We didn't have a lot of mobile apps even 17 years ago. The trust factor was really turning on the television at night. And you'll remember Dr. Donald Lowe, who was the chief of microbiology at Mount Sinai Hospital, where I was eventually and looking to him, the public was looking to him for good information about SARS. We've been doing contact tracing manually, historically, for years for centuries. And what has changed is this opportunity to do it from this technological point of view. I would also just add Chris raised such an important point about consent and then said, you know, what does it really have to do with cyber security but it but it really does because he gives these great examples of Will I be allowed into the park? Will I be allowed back to work? Is this going to be a condition adopting contact tracing in terms of reopening the economy? That's where Lena started. I think of it even in a health context where you can you can always model consent as choice and then you will be told Well, you, you have the choice. You just don't have to enter here. But we have to go back to work. As Chris said, you don't get paid. If you don't go in. I'll take a health example. And the visiting policies in long term care and hospitals, for example. The choice would be submit potentially if this proceeds, or you know, show us show us what you have, or you don't get to come in, but that's still your choice, but for many people going to work. Getting out into the community going to visit an elderly relative or whomever feels like more than a choice, it's somewhat an imperative. So there is definitely a need to be thinking about the

model in every, every jurisdiction is waiting through this and looking for some path through in that appropriate balance of what we ask of people how transparent we are, what data governance fits, and sits behind it. And then how we proceed from here. So I think this is a timely important conversation and I'll only just say I don't think it's, you know, I'll invoke and glucans language, it's not zero sum. I've seen some quite strident articles saying you can't have both you can't have privacy and then do contact tracing. I think we need to be very thoughtful and roll up our sleeves and and get that done in a way that will work and need is the mother of invention.

Lena Trudeau
It is we're here. love how you position that, Mary Jane ,as not a zero sum game. This isn't this is a time when, because of the need and because of those critical, what seemed to be trade offs, but back to your point for people, for many people in the country and in the world there, it's a false choice. And so how do we ensure that they're included in the decision making and that they understand what trade offs they're being asked to make? And that from a policymaker and an implementers perspective, we're doing everything we possibly can to ensure the security and the privacy and the good governance of the of the data and the infrastructure. I think, very well said. I'm going to turn next to Brendan Dowling and Brendan is with the Australian Government with Home Affairs, but he's actually sitting not that far from me in Washington, DC or all over the place right now. But Brendan and I are sitting in and around the DC metro area. And Brendan has a really great set of experiences from the work that the government of Australia has done to mitigate the spread of COVID. And so maybe from a bit of a, an experiential perspective, Brendan, you can talk to us about the importance of contact tracing and some of the things that you all have thought about and are thinking about as you actually apply the technology.

Brendan Dowling
Sure, thanks Lena. As Lena mentioned, I'm from the Australian department of Home Affairs, based in DC, but also working with Canadian colleagues very closely, I have responsibilities around the polar Americas region. So I'll talk about Israelis experience with contact tracing, and the deployment of the COVID safe app in Australia about five or six weeks ago. Yeah. I think the policy considerations are a really important place to start. And I think Mary Jane kind of covered some of the key ones, which is that in order to enable us to essentially open up the business again and for recreation and community activities, again, Australia is in a pretty good place. We've managed to control community transmission to a pretty effective degree at this point. So we're seeing restrictions aids, but the two major efforts of government to control second waves third wave, the next pandemic are really around testing and contact tracing, contact tracing, and the use of personal data to achieve contact tracing, our age old and those questions around data governance, the protection of privacy, our conversation today really important outside of the use of any app, the conversation needs happen around hospital data, how that's collected and protected. And so we're having we're having the conversation around how the apps can be useful in this exercise. But those fundamental questions are not are not specific to the app. So contact tracing has always been a part of what we do. And we'll continue outside of the apps to be what we do manual contact tracing. for Australia and for most governments around the world is still the most effective way to determine how many people in who have been diagnosed with ours have been in contact with. But to get to this specific so the COVID safe app in Australia has been downloaded by more than 6 million people over the last six weeks, which picks up a bit more than a third of smartphone

users in Australia. The two key questions I think, for us as we developed and deployed the we're really around functionality and community competence. So the functionality question is, does it work? does it add anything to the contact tracing picture in Australia, and to, there is no point in developing this sort of technology. If there's not community competence, there needs to be critical mass of people who are willing to download it and to use it and receive benefit to themselves and who see that their privacy is protected and information is secure. Because without that critical mass, it essentially doesn't achieve anything. So, like candor, and like the US were a federal system. So not only does do we need to get we need to build up some degree of community confidence in the use of the app. It relied entirely on state and territory, governments also being willing to participate. The health system is run by the state governments. So they are the ones who are doing this contact tracing. They're the ones who the data is useful. But without the state and territory governments of Australia being on board, then again, it's a non starter.

Brendan Dowling
As we developed it, I think one of the important decisions that Australia made was to basically forget about anything but the core functionality to say, this is about contact tracing and about identifying people who've been proximate for a period of time to someone who has been diagnosed as positive. So immediately forget about using it to enforce social restrictions, forget about using it to monitor where people are, and whether you've been subject your quarantine order will live at their house or not. And I think that was absolutely pivotal to the competence in the community. I think if there's a sense of what is this being used for is is being used for other purposes. I think you can forget about that. That sort of community competence aspect. So those two things those other elements, I guess, were dismissed, dispense with early on. It's not to say that, you know, some governments elsewhere will consider that there's value to those sorts of things. But I think there's a big trade off that you'd have to contemplate on. He did contemplate that. And how it works is that when you download the app, you are asked to input four pieces of data, your name, your age, your postcode, and your phone number, which is really about and the name can be pseudonym, it doesn't have to be your actual name. The age is about triaging. What are the most critical cases if you haven't large, lots of data coming in? postcode, obviously to figure out where the relevant health authorities close to you and phone number to a neighbor need to be contacted that future that to do very briefly going to be technical aspects that generates a unique identifier which then matches with other Bluetooth devices that you come into contact with the the app wakes up the Bluetooth on the smartphone every minute. It does drain people's batteries, which is being a big cause of concern. And it looks for devices in the area where it can match unique identifiers. Now, importantly, nothing happens. There's no notification to someone, if I was in close proximity to someone for 15 minutes, I don't get a notification saying you've been need someone who's been diagnosed positive with the bars so the user doesn't get any sort of notification. If someone is diagnosed with the bars and they with a medical professional, they'll then be asked whether they have the app and if they do at that point, a unique issue. SMS code is generated, which enables the data from their phone to be uploaded to, to the cloud, which is being run by Amazon Web Services. At that point, an algorithm does see. And you'll note, I'm clearly not a technical person here. So excuse me if I use any of these terms incorrectly. But the algorithm basically looks back through the data, the app is collected, and identifies people who have been in contact with that person for more than 15 minutes at a range of 1.5 meters. It's proven to be pretty good. It's not perfect at identifying, you know, whether someone's on the other side of it in wall or something like that. But it's proven to be

pretty good at actually identifying Yes, this person who's been in close contact for a period of time, over 15 minutes that if there has been those contacts, those contacts then go to the medical board professional as part of that health authority, and they then initiate the manual contact with the people that have been identified through the app. So at no point, does anyone except the Health Authority access any of the data in relation to it, and they can only access the data if there is a positive diagnosis on that person, which then enables him to do effectively the next manual steps of contacting those people. And I think the the utility of it is, is absolutely a really critical question here. And I think what we're finding so far is that it's it's useful when compared to manual contact tracing, where you sit and ask someone who have you been in contact with for more than 15 minutes in the last fortnight, but it's not a substantial sort of difference, that app is better. Then that conversation with someone, but it's not like we're finding out you're only identified half the people you were in contact within the app identified double that. It's more, yes, you identified most of the people. But actually, we think there's a couple more people that you're in contact with through the app. So I think our experience so far is that it's a useful tool. But it's only one part of the response. And as we look to the next phase of our COVID response, as we look for preparing to, I think, you know, aim that there are second wave, third wave that you can localize social restrictions rather than having statewide or national restrictions, I think we will find it a useful tool, amongst other restrictions amongst other manual tracing efforts and amongst people just moderating their own behavior. So it's part of the response, but it's not the sole way that governments are going to need to respond. So that's the that's essentially our story sort of six weeks into contact tracing. I should have mentioned at the start that ours was inspired by the Singaporean approach. They shared some of their approach with us, but then it was developed in house by the Australian Government. So I will leave it there.

Lena Trudeau
Brendan, thank you very much. And it's it's really helpful, I think, as we consider going back to those questions of, of governance and data management and security with respect to this, to understand the functionality a little bit better, because that specificity helps us really understand what benefit what return we're getting for potentially the trade offs we're making. I would call out, you know, earlier in your comments, and we'll get back to this a little later in the session. You mentioned that the fundamental questions of governance and data management has always been part of the equation. And yet, it does seem like the application of technology particularly in the case of some of the data that's potentially being collected and held, really takes this to another level though it's it introduces concerns about access to that data when it's distributed across mobile devices. And, and it brings that security that cybersecurity aspect into very clear focus pretty quickly. So we'll come back to that though. Thank you for raising those issues. I appreciate it. And, James, I'm going to go to you James, for everybody. James is the co founder of an organization called COVID. Watch, which is really looking at more of it if I understand it correctly, James, more of a public private model for doing some of this work. Can you can you tell us I mean, stemming from your work at Waterloo, where for everyone's information. James is pursuing his PhD in mathematics. You know, you're looking at alert technology, you're looking at other technology partners, and you're looking at academic partners as well as a means to scale the adoption of this technology, which I think we all agree if it's going to be effective usage that that ability to scale is going to be really critical. So James, over to you maybe to contribute a little bit here.

Lena Trudeau
Yeah, that's right. Um, so I think covered watch started sort of with the goal of building the most private technology that can still meet epidemiological needs to be have.

James Petrie
So I think from the beginning, we're like an academic, nonprofit with a number of volunteers where we're trying to develop the technology that allows us to do this and we evaluated a few different mobile technologies. GPS was one of the first ones we thought of and Bluetooth quickly became one of our favorites. So I think there's a few different Bluetooth sort of architectures that we sort of considered. There's the one being is a number of places, Australia, Singapore. And I think we considered something like that. But we found another model, which is called the decentralized Bluetooth model right now, which we found had quite a few good properties, because I think our goal was to be able to let people who download this app do so without losing any privacy at all. So in the decentralized model, the It works very similarly to a decentralized model. But the each device is emitting these random identifiers, but they're not tied to your, your identity there, random values. So when somebody later reports that they're sick. It's not a central server that checks if there's a match between these identifiers. These identifiers are distributed to each of the devices, and everything stored locally in your own phone can check if you were in contact. So this sort of allows us to do the whole exposure notification technology process without having to have any trust in a central authority. And I think that that's important in some countries, because being able to do this, getting the adoption will require a lot of people to buy into the system. So COVID watch right now is focused on running a pilot in the University of Arizona, and hopefully scaling up to the state there. But our focus right now is on demonstrate demonstrating efficacy. And also just Building Community Trust in a solution like this. Cuz even if the technology is very private, it's we have to show that we can manage it properly. And we have to be able to communicate how it works and why it's going to, like accomplish the goals that we have.

Lena Trudeau
Thank you very much that we keep coming back to this notion of trust plus advocacy is really the key to the whole equation. We're going to um, to move over to Sylvienow, Sylvie Frigon is with public safety Canada, and, and very focused on cybersecurity and the security aspect of issues like this and others, so maybe Sylvie, just to just to bookend our introductory comments, maybe you can share a little bit about how you and public safety Canada are thinking about it.

Sylvie Frigon
Thank you, Lena. To start with, these are mostly my views. So public safety is not officially involved in any work directly related to developing or choosing or evaluating any contact facing apps. Our focus is very much on the Internet of thing, cyber security. And it's one of the aspects that I'd like to send maybe a few, a few ideas to tomorrow to today's discussion. And I'm a policy person, I'm not a technical person says, you know, we tend to come up with a lot of questions and eventually get two answers, but usually it takes us a lot of discussions before we get there. So this whole discussion about the cybersecurity aspects of contact tracing are starting to emerge. And, and you're the previous panelists have identified some of the bigger questions that we've been been asking ourselves generally for internet connected devices, when people don't trust apps, when people don't trust technology, they will just simply not adopt it. And that does bring whoever is putting that ology out there. With, with the the

onus of securing those devices. There are very conflicting pressures, you want to get something to market quickly. You want to get something to market securely. And very often, it's very hard to do the same at both at the same time. So it's all about finding that balance. Now, if you don't get it right, then a lot of things go wrong very quickly. So if you introduce something very quickly to market, but it turns out that it can be exploited. And if we're thinking about something like contact tracing applications or just digital contact tracing in general, the the capacity of attackers to just get into that system falsify results, being people that you may have been in contact with telling them that you know, so and so has been positive for COVID-19. And they click this link to know what to do about that. And suddenly, you've been, you've been smished, your credentials and personal information gets stolen. So that's one of the consequences that can happen when you rush through the testing phase of things. Vulnerabilities in cell phones are being exploited more and more by by individuals with malicious intent. Cell phones have been compromised in use and become botnets that further fill for defeat into more compromises and ongoing data stacks maybe on health facilities, so on those aspects do are very negative consequences. I think it's been said that weak security can and will very likely limit the public trust and reduce the adoption of any technology. So this defeats the purpose of having it in place and first, first place. One last stuff, maybe on cybersecurity generally, is that as much as we were just talking about centralized versus decentralized applications, even the most self contained application that resides on your cell phone that is, perhaps itself encrypted, very strongly defended, will only be as good as your capacity to update that application. So any update that's pushed by a publisher or government if it's centralized by health, it will necessarily mean that your cell phone is open to the outside world. So security is never static. It's only as good as it can be updated for new threats and new vulnerabilities. So it's it's probably another very complicated issue to just make sure that don't only have point in time, right now security, but an ongoing way to keep any connected device secure is, is a very big challenge and will continue to be. So with that, those are just a few considerations that are both in my mind, I think we've had some excellent discussions, a lot of questions already. And I keep my remarks to that for now.

Lena Trudeau
Thank you so much for sharing that. And we're getting some great questions in from folks who are tuning in to this event online, and I will we're, we're looking at all of them and I will ask, I'll try and get to all of them, but I'm going to employ the moderators prerogative and asked a couple of questions of my own First, if you don't mind. But thank you for that very informative sort of context setting. And we've talked about, you know, the concept of contact tracing what it is the the value that it could potentially provide, when deployed Well, some of the functionality, some of the examples of different models that are out there between the one that was deployed in Australia and the one that James is working on, out of the University of Waterloo. I think all of that's been really, really useful. I guess the question, you know, thinking through what Sylvie just said about, you know, one of your comments Sylvia was about the tension between the push to get something to market and the desire to make sure that it really is thoughtful and secure to some extent harden before it comes to market. I mean, in addition to the regular commercial pressures that you will see in, in technology launches, we're really talking about the ability to prevent or mitigate a second wave here, which is a really serious issue with a lot of urgency behind that. And so I guess my question is, rather than talking just about the risks, I'd like to understand from each of you if you could contribute some thoughts on what mechanisms we can put in place to ensure greater security as we bring these capabilities to market. You know, we've talked about the

need for for trust, and of course, that takes time and engagement and, and discussion and conversation, but it also takes some ability to credibly describe the security measures that are being put in place and ways that people can can trust that there very private information, health information will be kept safe. Does anyone have thoughts to contribute there on what, what we can do as we bring this to market to ensure that not only are the applications and the data, privacy and security issues addressed, but the people understand how that's addressed, and they have the capacity to be able to, to then place their trust in something like this. Okay. A comment on that, please, James.

Chris Parsons
It's Chris.

Lena Trudeau
I'm sorry.

Chris Parsons
My apologies. No, my apologies.

Lena Trudeau
I apologize.

Chris Parsons
James, go ahead.

James Petrie
You go first.

Chris Parsons
I just wanted to state that this is fundamental. This is in many ways, fundamentally a biosecurity issue. So you know, the way that it's been framed. Yes, it's a technical -- Do we have the apps written properly? But this is a question of, can we secure the population at large, from, you know, pretty pressing and serious threat is living with us right now and will continue to live with us for, you know, months or probably years until treatments and vaccines are available. So one of the ways that I think it's it's really critical to work through this is not just having the application secure, which matters, not just having the phones secure, which is very important, not just for the app, but everything else. But we actually need to convince Canadians that we're probably going to have to shell out as a population. And this is true of other jurisdictions as well for mobile phones or other tracking devices. And that means that we have to go into communities that are disproportionately affected by COVID in terms of hospitalization and in terms of mortality. That means going into black communities, that means going into Aboriginal communities. That means going into the places that are historically disadvantaged. And we're not everyone has an up to date phone or phone that can receive contemporary updates. So we have to get the applications, right, we have to get the distribution of the means by which we can actually install those applications right as well. And that means that if we're going to address this, it can't just be how do we use the tools that are available right now? Because we know that many of the groups that will be most effective don't have those tools. And so how do we convince seniors to use

these devices? How do we explain how a phone works or a tile based tracker or something like that? If we don't get those questions, right, which kind of broader public policy issues around biosecurity for use applications, then we will protect one segment of the population that tends to be more privileged, while simultaneously not protecting other segments. And we know that this isn't a disease where we can affect one group and no one else. We're not all within a similar protective cloak, we will, infect one another. And we won't be able to use the apps to notify people in black communities, Aboriginal communities, or frankly, in mixed communities where we have lots of different socio economic groups, you know, wandering amongst one another, the apps won't know that someone over here who doesn't have a phone was near me and I did have a phone. And so, that will also cause some difficulties. So I think that we need to, again look beyond just the application and look to the the broader conditions under which an application is even possible.

Lena Trudeau
Thank you, Chris. James, you had something you want to share as well.

James Petrie
I'd like to second what Chris said, and but yeah, ensuring that this technology which is everyone is like super important, like in terms of equity, and also in terms of like, like, effectiveness. Like we've done a few models or simulations of this and it assuming everything is modular. This only goes so far. If you have a small subpopulation where you aren't protecting these people, the pandemic just keeps going. But to address the first question of like, how do we, how do we actually convince people? How do we build trust, the covered Watch has been taking a few, three different approaches, sort of. The first is, we're open source, we've always been open source. So people can look at what we're doing. See how everything actually works. Second is we're going to we're going to get third party security audits, to make sure everything's actually implemented properly, and someone actually signs off that they've looked through everything. And then in terms of public trust, I think one of our partners actually had a great metaphor that I liked two days ago for how to explain the technology and at least far system sort of works like a like, you know, like raffle tickets with like, you've got two, two numbers on each piece of paper, you hand them to people. For the decentralized model, it's like someone gave you a big roll of raffle tickets. And everyone you pass by you just hand them one of your tickets. And then if you become sick, you just broadcast your other half the tickets and people check on their own. So I think using metaphors like that, to sort of like, really convey how the technology works, and how actually you're not really losing any privacy, if it's done properly, can help with adoption.

Lena Trudeau
Thank you. Very plain language, and descriptions are really important, no doubt. Mary Jane, maybe you can comment a little bit on the consumer public perspective.

Mary Jane Dykeman
Yeah, and I think that follows on from what James has said that in ultimately, even when we talk about modernizing existing privacy legislation, and pre COVID, we've been quite focused on a new element. It's an element that we certainly were mindful of, of public sentiment back in the mid 90s, drafting house health privacy legislation in Ontario, that many jurisdictions are starting to modernize. And they're having active conversations about how we engage the consumer. We have health consumers who

want to have all their health records on their wrist. So to the extent that people are already wanting more of their information and to hold it, we've been talking for some time about, well, how do they do that securely? What guidance do we give? How much autonomy do we give? It's not to say that that people wouldn't be allowed to have that information. It's it's actually their information, but in terms of creating a framework, how do we put that narrative out so people can help themselves. And it's the same discussion we've been having during COVID as everyone went home to work, so work from home already meant that people were using personal phones and devices, and there was a bit of a scramble and a flurry. So if we're going to extrapolate and talk about enabling and people's phones, and possibly a decentralized model, which from a security perspective, gives you a little pause, what is the trade off, if it were centralized, it might be easier to make things secure and put a big gate around it, but then data ambition comes forward later. And downstream. Somebody else may want to use the data. So I think there's a real question of how we engage communities so that people a know what contact tracing is, know the parameters, know how they can help themselves. Is it going to be voluntary? Is it going to be imposed in some way? Just Just so that we're also not asking for a consent if it's not a consent matter? Again, those are things that that are coming, that I think it's important to think about that narrative. Now I've said for years, we need to tell a better story. And this is not a made up story is not a one sided story. But we need to engage with people and get that balance of giving them the appropriate correct information, as much as we know it in enabling them to also help protect themselves and if they have choice and to be clear about those choices as we bring this technology on.

Lena Trudeau
Thank you for that, Mary Jane. Brendan, I don't mean to put you on the spot. But I'm really curious as to how some of this has played out in the Australian context, this notion that Mary Jane speaks of putting a framework in place is a very, you know, thoughtful and transparent approach. The the ability to engage with communities, particularly underserved communities and communities at risk is really important work. But all of that takes time. You've been, you've sort of been part of the experiment in real time. What's the reaction been like?

Brendan
It's really, really interesting. And I think we, we've all touched on this. He plays into much bigger policy questions at all that governments are grappling with at the moment about the use of technology about data protection, which I don't think any of us would would claim that we have the balance struck the government's tech companies have all failed in terms of cyber security protections in a myriad of ways. We had a really interesting debate a couple of weeks ago in Australia about the digitalization of health records, which, from a medical perspective is a really helpful thing that you can go to different facilities and they're able to access your health records. But there was a huge negative reaction about how people's medical information going to be protected. So I think this, this debate plays into that much broader debate. But I think the difference with the situation under these pandemic is that governments and the community have sort of cold on each other to in ways that I don't think we've seen in any of our lifetimes where you've had, you've had governments standing up and saying, We need the community to do to behave like this. We need you to self regulate your social interactions, the way that you behave when you go outside. You know, everyone kind of has to step up he and behave in certain ways that mitigate the spread of the virus. And in most respects, you've seen communities respond in a really positive way to say, Yes, we will do that we will not go to parks, we will wear a mask, we will do certain

things. And I think that sense of community engagement probably helped the take up of the app in Australia, in in vast numbers. It's not to say that people were willing to do it and say, Okay, forget about privacy, forget about trust, you know, we're on board, we're going to sort of simply plain to these, those expectations with their bills, a lot of questions, asked about data protection, what the app would do, I think simply explaining the apple doing this, and it won't do that. And here's how we're going to protect your information and insurance not accessed by the police insurance not access by the border force. People wanted that to degree of assurance. There was a negative reaction to the fact that the cloud provider for the app is Amazon Web Services. Which is a US based company, in the sense that, does that mean that US authorities will be able to access data about Australians. So people did want that degree of assurance. But the rapid take up, I think, I'll get this slightly wrong. But within 48 hours, more than 2 million people had downloaded the app. So I think, in the peculiar situation we are in at the moment, you saw people willing to make a leap of faith, because of the potential benefit to mitigate the spread of the virus? You know, why? I don't think we would have seen put us on the pandemic and you ask people, you know, the government's got a new app, we wanted everyone to download it and input their personal data, you know, as quickly as possible. Forget about it's not, it's not going to happen. So, you know, we have those broader questions which we still need to resolve between the community between the government and the tech industry, but some of them I think there was a greater degree of faith. than we might otherwise it's saying because of the circumstances we're in. And just to briefly touch on, I think the less privileged communities, communities that don't use smartphones as frequently. I think that's a really, really important consideration. I don't think we've solved that. I think that's something over time, you might work to expand the availability of devices, you might look to educate people who aren't as familiar with them. But I think you also have to accept that there are a bunch of communities where you're not going to be able to do that in the short to medium term, and you will have to rely on other methods, manual contact tracing, etc. to achieve the same end, rather than hoping that you'll get these whites this this universal dispersal obvious of the technology.

Lena Trudeau
So it goes back to the notion that you were raising earlier as well. In your opening remarks, Brendan, where, you know, the technology is useful but it is not a panacea. It's not something that solves the problem entirely. So we're talking about this as a tool. That is one of many in the toolkit. But this has to be a sort of multi channel multi model, kind of what exactly. Got it. Okay. That's really helpful. Thank you. James, I want to go back to something you were saying about the way that you deploy the technology. And I'm going to show my bias here a little bit by saying, I think sometimes large federal bureaucratic organizations aren't as well equipped as maybe some folks on the front line of the deployment of newer technologies to understand what's really possible. And when you were describing the model that you're pursuing, with covered watch, it sounded very much like it has elements of privacy that are embedded in the technical approach and so on. I guess and not to put you too much on the spot. But to what extent do you believe that the proper deployment of the right technology for this can go away as to addressing some of these concerns?

James Petrie
Um, like so to compare with the like, if the technology is private versus if it isn't private, and how that will, like drive adoption? Is that your question?

Lena Trudeau
Well, I'm thinking particularly of, you know, different mechanisms that we might be able to use to anonymize the data or protect the data in different ways. ways that your analogy of the band of dual raffle tickets and having numbers connect with one another route and be related back to something else rather than have it be specific to the, you know, the data and the individual combined at the same time, Is it? You know, it's a very simple analogy, but it's a powerful, you know, application of the technology. There's there are differential privacy pursuits or approaches that we can take with, with some of these, but I'm sure there are different -- there is capability in the technology that is changing all the time. And I guess the question is, in your view, how much of that does go some ways, at least to addressing some of these privacy and security concerns?

James Petrie
Yeah, I think we've been very happy with how the technology is developed. I think, like maybe a year ago, like at least if I'd thought of something like this, it would have been, everybody puts all of their data into one spot, and even even the models that people are calling centralized aren't even as centralized as that like. like doing it all like In a sort of decentralized way, where there's not some location that has everybody's GPS history for the last few months like this, like miles ahead of where it could be. So I think this type of development is very important for, like making sure that the things we develop now want us badly in the future.

Lena Trudeau
Yeah, it's a that's a whole other issue that we need to explore a little bit. But Sylvie, you know, you you raised a really good point earlier in your comments about the risks of things like basic phishing campaigns when people are using their mobile phone for applications that store or potentially store maybe just access important health data. To what extent do you -- we've talked about the some of the things that policymakers and legislators the people who are governing need to be thinking about in the deployment of this. But what is it that we're asking of people who need to be using these tools? Because it sounds like in this equation, they have a certain amount of responsibility themselves.

Sylvie Frigon
At so that's always a very good question. I think that any new tool will hopefully, if deploy, come with good sources of information its use and how secure it is. Basic awareness in cyber security is still very much a challenge in, in well, pretty much everywhere in the world, but in Canada as well. Even though we have a really high uptake for technology. We still have some basic messages that need to be reiterated, you know, don't click on the link, don't visit the website that promises you a miracle cure. Those questions have been raised even more in recent weeks with the number of COVID related fraud attempts and all those, those events that we've heard from the news and through which we're different government bodies even that are trying to really raise that awareness. So awareness is key. And just the general thing before you click is still the basic message, but you have to be careful and think things through and design them. So that it, you know, that solution themselves rely on being built securely, but also, it is possible for the average user to to maintain it that way, and to take the right steps to protect themselves, but that's still a huge challenge and from a technical perspective, I'm sure James would have a lot to say about that aspect of things much more than I would as a more technical person. But I

think that there's, there's still a big reliance on users for security. And unfortunately, that's not going to go away. So how do we deal with that? That's the big challenge.

Lena Trudeau
Yeah, and I know from my experience with the Government of Canada, that at the federal and provincial levels, there's actually a real commitment and resourcing behind educational programs and, you know, the, the ability to put better information and, and tools and frameworks in the hands of individual citizens who increasingly rely on technology. I mean, in this in this time of social isolation, and quarantine, and, you know, work from home, wherever folks can do that, where the work allows it. It's it's not just the question of health data, but you're right, a lot of other important data as well, that is at increased risk of being able being being accessed electronically. So it's a much larger question.

Lena Trudeau
It sounds to me like we're well into this conversation. Now it sounds to me like some of the main themes that we're hearing here are that there's a set of responsibilities on government and policymakers to engage with communities have this discussion, particularly disadvantaged or at risk communities, communities that contain more vulnerable populations, they need to be at the table as part of the conversation. So there's a real engagement piece to all of this. There's a transparency and communication aspect where being clear, and using as simple language as possible to explain what are often very complex concepts is going to be critical, making sure we get the technology right, there are a lot of models to choose from it sounds like and potentially pros and cons with each understanding the technology, constructing it properly and deploying it effectively is going to be critical. And then there are also as part of this overarching framework for how to do this more effectively, there's a conversation to be had with individuals about their responsibilities in this equation to ensure that they're, that they're adopting the application and allowing it to scale which will drive greater effectiveness but also that they're treating the application and the information with the responsibility that it requires. And so, I guess, looking across all of that, those are some really great you know, themes that we can take forward and share with folks in terms of how to deploy contact tracing more effectively. But then, you know, you get into this very interesting question. And it was raised by a member of the audience, about the use of the data. And James, you hinted at it, like, as we build out for this use case, as we deploy for this need. What does that mean for the functionality we're actually introducing and putting in the hands of powerful governments for what's next? And so the question from the question from the audience was really more around, how can we assure citizens who are sharing their data, that it will be used for this only and not shared? and appropriately, even if, at some point later, you know, we discover, oh, it could be really helpful from a public health perspective if we just did this. So how does that happen? Who can comment on To make sure that that there's trust in the way that the data is going to be used, not just collected and secured. James?

James Petrie
Yes. My answer to that is sort of like sandbox, our approach has been just to not collect it in the first place. So even if you'd wanted to use it later, you don't have it. So you can't.

Lena Trudeau
it sounds Brendan that the way that the Australian Government deployed this, there is a certain amount of collection. Is that true? Did you have to sort of identify the uses of that data and the limits on that?

Brendan Dowling
Yeah, I think I think that's, that's, that's the key to it. What what data are we collecting? What will it be used for? And how long will it be stored for I think, the, one of the key things that he mentioned is that the -- so as as the app is collecting data on the unique identifies with whom you've been in contact with. So it's not storing not collecting at this point, you know, bio data that self deletes 28 days after collection. So it's not stored on on the phone or in the app for longer periods. It also, I ran through the data that we collected, very sort of basic name, age, postcode and phone number. I think that's, that's quite key to how the public engages. They want to know what data you're collecting. And they want assurance that the app is not delving into other parts of your phone's data, including around location data and things, things like that. I think that you've seen the debate around Google and Apple sort of efforts, which is really centered around the location data. The, and that limits, you know, I guess the, even if someone, even a malicious government looking to surveil their population was looking to misuse these sort of data in the future, the fact that you haven't collected a broad range of data that could be exploited for other reasons, I think it helps to build that trust. So I think it really does come back to that, that answering those questions, honestly, and in simple terms to the public, what data are we collecting? And how are we going to store it and use it? And unless I think unless you can have a sensible answer and a simple answer that people understand, then you have that undermining of trust and the sort of undermining of potential take up.

Mary Jane Dykeman
Lena, can I also jump in I mean, I do find this fascinating because we're actually drilling down to the legal authority to have collected it in the first place. And often in these conversations, what's happening is we'll focus on what's the legal authority to use it, what's the legal authority to then disclose it. But we do have to go back to what was the authority we relied on to collect it. And in this case, presumably, unless it's going to be compelled, we were choosing these data elements and collecting with consent, and with a promise that the information then would not be used for other purposes. So the fact would be that you have a repository of information potentially, if you do collect it in that manner. And you do have to go back to the point of collection, the mere fact of just having it doesn't give that legal authority just because it's created. Now, I guess, you could probably invoke something in the legislation to then go ahead and use it but there's a nuance there where we can't just talk about the authority to use something or share it in some way. You have to go back to the first principle, what was the authority and the promise upon which it was collected. And Brendon makes a good point in that in his case name, postal code, phone age, those are not inherently personal health information, maybe a an app that deals with personal health situations, potentially. But even still, even with those data elements, what was the authority to collect it? What did you tell me? So I think I think we've got to consider that there'd have to be some sort of legal instrument or authority that is brought forward later. And it's not to say that someone could not pass up but it's just not something that people could do automatically.

Lena Trudeau
It's so interesting, and then it comes back to the question as well. Mary Jane, of. and you raised this right at the beginning, there are voluntary models. There's models where you could compel people to sign up for a contact tracing app or provide a certain amount of information that's personally identifiable. But there's also this gray area in between where practically speaking, if we're making public transport and earning a wage dependent on having an app like this, then to what extent is it really voluntary versus compelled?

Mary Jane Dykeman
And is it voluntary when you ask my permission, and I give it to you, based on your promise that it will only be used for limited purposes, so we have to be very careful. Again, if there's that data ambition later, I worry a lot about those downstream, inadvertent or malicious uses. Where it's, it could be two years down the road, it could be in not just the next wave but another pandemic and even in Ontario with the recession. To see management Civil Protection Act, which is just really that set of orders that governments allowed to make, they gave themselves very broad authority to compel collection of certain kinds of information. I don't know that they have relied on that regulation. they've they've done all kinds of other orders during COVID. But at the same time, they put certain parameters that would protect from this information going downstream, used for limited purpose, not then put into someone's health record, for example. But there's always that potential of the attention turns away, there's a great repository, there's not a lot of memory of the why or how or for what purpose and someone might have, wow, it's really great idea. Wouldn't be great if we could use this rich data set to do X, Y or Zed. But I still back to what was the promise we made when someone decided to share those elements that that Brendan's talking about or maybe other elements that other governments see fit to include.

Lena Trudeau
What's so interesting, I agree with you. It's fascinating, what's the role of the business community here. So I'm responsible for a workforce and we're very fortunate at my firm to be able to work in a distributed way very effectively. So, having said that, though, you know, as we look at reopening our offices and putting the right sort of physical distancing and cleaning and hygiene and other safety protocols in place, you know, there are guidelines that are coming out from places like the CDC, that that recommend taking temperatures and doing some other work to ensure to the extent possible, that folks are not, are not infected when they return to a physical office. We've talked about governments and we've talked about individuals, we haven't really talked about the business community and the implications legal and other. If, if the business community was to, for instance, not require temperature taking or not require something like contact tracing, and then people in their organization, in fact, others, there's a potentially illegal liability there as well that I hear a lot of folks talking about. And so there's this, there's this real tension between personal privacy choice concerns about legitimate concerns about security of information, and, and the practical reality of what it means to actually begin to bring people together in close proximity. Again, I don't know if anybody's having those conversations or if there's a perspective on this panel on how to how to engage the business community around this I, I wonder if they can be helpful.

Chris Parsons
I have something to say on that. If there's a moment.

Lena Trudeau
Thank you, Chris.

Chris Parsons
Um, I think one of the there's a lot of different variables. So I think CDC guidance and obviously following health authorities are putting out it's going to be essential in order to build a safe workplace, maybe legislative measures that are helpful in terms of identifying liability. But I also think it's important about ensuring that the tools are in place to empower individuals to not be at work if they think they may be sick. And so in the Ontario context, which is the jurisdiction where I happen to be residing at the moment, you know, paid sick leave isn't a guaranteed element in your employment contract and moreover, where it is there, it may not last as long as you may have to self isolate should you have COVID. So I think to begin with, we really need to think in the business community, how can we not just build our spaces that are safe? But how can we ensure that employees are able to behave responsibly in a way that doesn't threaten, you know, again, their ability to put food on the table, or pay their rents. In the Canadian context, we're seeing some proposals from the federal government around, some of the emergency funding might be available to take up to two weeks off. But again, that works well for you know, if you live alone, in a home, but if you have children who are going back to school, if you have a spouse or partner who's going to work, you may have multiple boats where your whole home has to go into quarantine. And so figuring out those pieces, I think, is as important as figuring out the actual you know, how many people can go into an elevator and frankly, is it even possible in 40 or 50 storey building where you can have four people in the elevator you know, would -- if we ever phones coming back to the office space? Does that mean that by five o'clock, it's time to start sending people back down because we finally got people in their offices. So I think that there's going to be a lot of assessments of how to do the physical elements. But I also think it's important to think about the employees and how do we empower them to behave responsibly and safely and not want to cheat any mechanism that's been put in place?

Lena Trudeau
Then I could also comment on that liability, please component because I do think we're seeing some things that will be concerning already. In the business community, everyone has returned to work on their minds and what happens if there's a second wave, but we're already seeing some lawsuits being filed and some successfully already, in terms of things like personal protective equipment, so PPE, nurses in a long term care setting saying that they weren't given enough or weren't given it soon enough where it was being held back? I hear organizations saying already, Well, we're just doing we're following very closely what the government is telling us and monitoring for reports and everything else. And I do think about two post SARS and the commission that looked at the SARS situation, what did organizations know? When did they know it? Health care workers died and the late Mr. Justice Campbell, did this Folsom Report and it didn't point to the peril of relying only on the guidance that's coming. So I do think that there's a certain anxiety within the business community who say every lawsuit is going to be successful. But if I extrapolate again, I take that parallel from the PPE situation. Chances are we will see lawsuits that said there was something available and you did use it or you didn't use it. And we may certainly see some of those suits being filed. And then the other corollary is the fact that we're also hearing that insurance is potentially going to be limited to cover COVID related

situations. So, we're at a real crossroads. I think, obviously, we want to get the contact tracing, correct to move communities back into work and back into all of the things that that they wish to do with all of those balances, because I'll be the first to talk about the privacy and the governance and everything else. But there are real questions on the minds of business owners as well, not just their day to day ability to operate their businesses, but the net impact of of potential suits in occupational health and safety. So I'm glad that that was also raised.

Lena Trudeau
Yeah, it's such a complex issue. There are -- listening to all of you with your expertise, it's -- the one thing that is striking is that there's no clear path where it's easy to say that's the right way to go. So I guess, I guess my question is, in the context of all of this, is the deployment of contact tracing technology -- is the juice worth the squeeze? Should we be doing this? Does anyone have a perspective?

Mary Jane Dykeman
Only to say I'm going to work that expression in too many legal arguments? Is the juice worth the squeeze?

Brendan Dowling
I'm happy to. I guess it's from our perspective, it's a qualified Yes, at this point. And I think and I've noticed a couple of questions coming up from the audience around the effectiveness in Australia. The reason I think it's qualified for us ease, we where we're at On the on the sort of infection curve is a really kind of positive situation at the moment. So I don't think we necessarily have the critical mass of data to say, yes, this has been a game changer. For us. I don't have the data on how many cases the the app has been used. But to give you a sense of the current situation in Australia, so in the last 24 hours, we've had two new cases diagnosed with divorce and both of them have been in international quarantine facilities after trickling in. So at this point in time, we don't have the the caseload of I guess transmission, where the tracing app is making a, you know, significant pivotal difference to how things are playing out. However, I think where we'll really see the potential value and this is slightly speculative is when you get to those future outbreaks. What the app does is increase the speed at which you can identify the contacts that someone has had. So does it allow you to pursue rapid, localized restrictions? That means you can essentially jump on an outbreak much quicker than you would otherwise have been able to. And I think what we're going to save the second, third, fourth, whatever ways we have, is the speed at which you can identify and localize an outbreak will make a significant difference to how much that spread then happens. So I think our hope is and where we, where we sort of are continuing to, I guess, work to improve the app in Australia, is that it positions you to deal with things in a much quicker and localized ways as you see those future outbreaks. And for me, that's what it achieves for us, then hundred percent that's worth it. Now, does it? Does it do that? I think, you know, it's gonna be some time before we see the deep analysis that says right he's here The fact is that enable these different countries to control things in these different ways and definitively answer those questions. But the potential to rapidly localize restrictions I think is very much worth it.

James Petrie
I'd like to add that in that. There's like the real world stuff. And then like in the simulations like it if you get to like a 80% 90% adoption, like, huge results. But that's, I guess there's a big divide between what the simulations say, and then, like what actually happens, like when people use the app, will people follow advice from the app. How quick, how much testing are we doing? There's a lot of questions to solve in the real world to know for sure.

Lena Trudeau
Yeah, absolutely. And, you know, I could certainly see cases where it goes back to that issue of trust. We're in areas where there's low trust and institutions, that there could be, you know, a rejection of that or where there's not been the work done in advance that hampers the adoption. It hampers the effectiveness as well. But all of this is really helpful context. Does anyone else want to comment on this question?

Lena Trudeau
Okay, my follow up to it then is, you know, as we think about what's next, if you could wave a magic wand and make one recommendation to your policymakers, who are considering, you know, whether and how to deploy these kinds of capabilities? What would it be? What would your, you know, what would your ask be or your strong recommendation be for something that governments need to be? Either absolutely. deploying or exercising or strongly considering, really, really thoughtfully as they look to whether or not to deploy these kinds of capabilities.

Brendan Dowling
I'm happy to have a go. I think the fundamental question that every jurisdiction needs to ask is, what do they want to use it for? And I feel that the the fork in the road moment for us was deciding this is going to be a better tracing proximate contacts, and it's not going to be about anything else. And that sort of answers the next questions of what data do you need? How long do you need to store it for? I think you'd be trying to use it as a measure to enforce it, adherence to restrictions to use it for for entry to public transport or to workplaces, things like that, I think, you know, increases identify a few sort of critical areas. It's not to say that those, you know, they may have value, they may be worth the conversation. But I think as soon as you make that choice to use it for broader purposes, you're going to get a massive trade off in the buy in and the complexity of the questions that need to resolve. So you're looking at speedily deploying something that does one thing, then then focus narrowly on that, and don't try and have it so all your coronavirus related plicy problems.

Lena Trudeau
Thank you, Brendon. That's really insightful. Chris, from your research, what do you think? I mean, you were talking about the issue of engagement early on, but like, I guess the question is, what would you recommend legislators in Canada in the Canadian context, consider as they, as they think about whether and how to deploy contact tracing.

Chris Parsons
So if you'll correct me two pieces, one of which, I suspect, Sylvie may be better equipped to respond more comprehensively. First, I think that we need to think beyond the security properties of any

application. The lab we actually just published today a case of an international hacking group that uses incredibly efficient phishing leads. We know that as soon as applications are installed on devices, and once bad guys know what alerts look like. They are going to start figuring out ways of setting those alerts to individuals. So Korea has a system where you can access it, publicly available in English, that they did a public campaign. This is what our alerts look like, here is how you will go through this. And so you have to have an education campaign, not just around how to install the app, but also how to respond to all the data that's on technical security. That's where I think it's important. The other thing is, I think that there's actually a community in Canada and frankly, all around the world that has and is dealing with a serious disease and has been stigmatized in the past. And that community has developed its own solutions. And it also has its own very clear attention, awareness of the risks and dangers and how states can collect data, save real insights to share. And of course, I'm talking about the gay community with the HIV and AIDS epidemic. So if I were talking to legislators, I would want to tell them be very, very, very, ceratain, that you have members of that community in there right now, what happened, that maybe it was well meaning, but went wrong in the past, because those are groups who have been under health surveillance. These are groups that are historically disenfranchised, in public health responses. These are groups that can really teach us a lot. And so I don't have what they would say because I'm not a member of that community. But I think it's one of those situations where that's a community that has a lot to share, and not just in how to deploy a tracing app, although that's going to be important. But also how do you develop a resilient community in the face silent and invisible epidemic that's just spreading through your community and killing people? How do you build resilience? How do you build joy? How do you move away from I'm scared of the world, too. I love the people that I'm around and I think that's an important component. Fear will drive people to do an awful lot of things as we know, but it's a short term motivator. And so we need to work with communities that have dealt with fear and engage with fear and have moved beyond fear. I think that the gay community in particular, will have real insights that will produce a huge boon to our legislators and thinking through appropriate effective public health policies.

Lena Trudeau
That's very, very interesting. I hadn't thought of it that way at all. And back to your, one of the very first points you made, the black community, the Aboriginal community, the pardon me, the indigenous community, often at risk, and receiving, you know, potentially dramatically underserved in, in health services, so important for those communities, I would think to be involved as well. Does anyone else have something on their list of recommendations for policymakers?

Mary Jane Dykeman
I'm still focused on what we collect, what we tell people. And I'm already thinking, How exactly do you draft that, such set? No, it's either set, and we abide by it. Because there'd be nothing worse in a way to go forward with this. We know that we're not able to keep up with a manual contact tracing, that day really has passed, we have this opportunity. We can build protections in. But we don't want to make a promise we can't keep because if we are fortunate enough to garner that public trust, and then misuse it, then that is going to make it even more difficult in a second wave or down the road in another pandemic. So really, we've got to take that careful step not to stop because we don't want to impede but to do this swiftly. But carefully and with some rigor and following on what Chris said, I'm thinking of communities who've recently come to Canada who possibly have come from other places where state

surveillance is for real. And again, how do we learn from them and have take those concerns into account? that's a that's a large promise. It's one that I'm very confident we can keep, but it's going to take some vigilance, not just today is this thing launches and then we move on to the next thing, I don't want to call it the shiny things is much more than that. But really, if that's the promise, then that's a social fabric.

Lena Trudeau
That long term thinking is going to be really important for a number of reasons. Those that you've described, and James, you were talking about it in a slightly different way thinking through the implications down the road. Of what we deployed today and how we, you know, the the capability of the technology is very, very powerful. And, and I look at the fact that I mean, I'm sitting here in Washington DC and not to put too fine a point on it. But there are an awful lot of protests going on where people are in close proximity, and where the value of the contact tracing app might be both very useful and very concerning to people. So thinking through those implications that are downstream, I think will be important as well. Do you agree?

James Petrie
Definitely. Just making it so that there is no possibility of future surveillance, where it's like, building technology that we're not going to regret a few years from now, I think is really important.

Lena Trudeau
Yeah, hundred percent. And Sylvie, I'm going to come back to you just for a moment because I do think there are some very useful models that have been put in place around public education with respect to security. And, you know, if you wanted to comment on that for a moment, from your experience, I think we'd all benefit from it.

Sylvie Frigon
That's a really good question. Um, it all depends. From the perspective of the Internet of Things. As you know, that's everything that's connected comes with a lot of rewards and a lot of risks. I think we're still at that at that stage of waiting. It was -- and I also liked your, your expression area is the juice for the squeeze. And that question is not going to be resolved quickly. The models that are out there can give us good pointers, but everything we do has to be contextualized to what we want to do with those tools and what are the benefits and what's the specific Canadian context. For example, if we're talking about something that the government's here might be considering. Trying to go quickly through those questions, I think are going to open the door to longer terms questions. And James just mentioned, you know, what, what could and need to be used down the road for? And it's hard to answer those questions as policymakers. But I think it's our it's our duty to just think things through very carefully. I really, I really love how Chris, put this idea of diversity, and the experience that you can gain from talking to different communities. So, it's about cybersecurity. It's also about how to help people understand how to better protect themselves, in this context, where protection of larger populations is really what we're aiming for. And I don't think that we'll have one magic solution to all of it. For a while we're going to have in person contact tracing, we're going to have digital contact tracing, we might have -- I was reading just this morning about the idea to use smart, wearable technology. So, your Fitbit might tell you, at some point hey you might have been exposed? How do we build all of that into a

model that's going to become coherent down the line, while also protecting ourselves from whoever might be trying to, to attack us through all these new doors that we are creating with this technology? So there are many models, but I'm not sure that there are many answers at this point, and we just need to continue working through them I think as policymakers.

Lena Trudeau
I think one thing that is increasingly clear is this discussion around sort of contract between individuals and our Government is something that, although we're talking about the specific use case of COVID-19, and contact tracing, is really a much larger question about the role and use of technology in our society and the responsibilities on individuals on the business community on on policymakers and legislators to ensure that back to your word messaging, the right framework is in place to have informed conversations in, you know, among communities and between citizens and their government about how we're securing that how we're managing the, the use of data, the collection, the maintenance, the price, maintaining the privacy of it, and also just other aspects of the governance that we're putting in place around all of that

Lena Trudeau
Our goal in this conversation was really -- I want to bring it back to the security question specifically. But I do want to make it a little bit broader than contact tracing. If folks around the horn here across the panel might think through, you know, from a security perspective specifically, any final thoughts you have on this, this use case of something that could be so valuable in saving lives and helping people regain some sense of normalcy in their daily life? does seem like it holds a fair amount of promise. I guess I just would ask from a from a security perspective, because we at the Internet Society really do want to think through how we can further that conversation. Is there anything you would add that we haven't already discussed?

Chris Parsons
If I can. I have one small point

Lena Trudeau
Thank you, Chris.

Chris Parsons
So, you know, one of the groups that we're obviously most concerned about because of the fatality numbers are seniors. We also know in the Canadian, but not exclusively Canadian, context, seniors tend to not have a high penetration of smartphones and smartphone use. So, you know, let's imagine that smartphones are the way that at least these apps are initially deployed. And we really want to keep our parents and grandparents safe. So we definitely want them to have a smartphone. Now, that has a lot of implications, because we know, you know, I keep thinking about, can we secure the app? Let's imagine that's true. But there's all the surrounding security implications. So as soon as you give people who are known to be more susceptible to scams, to email phishing, to all sorts of harmful effects as they don't have the same digital literacy, what happens when your grandparent or your parent has a smartphone for the first time, all of a sudden they're getting information from places that are great, they're clicking links that you sent them, but you didn't send. And so it's I think it's really important,

obviously, that we think about how are we going to address the security issues linked to combating the pandemic? Fully agree. But we also need to look to see is the solution that we're proposing actually increasing certain fret registers for members of our society. to say nothing of the fact, you know, will this work? I think that actually the processes that responsible researchers are doing right now, long term testing, evaluation, seeing how you build social trust, that's the model to go with. Rally quickly running it out. I super understand, you know, you want to get something done. And this is a crisis moment. But this is also a crisis moment that, you know, depending on who you're reading, we're going to be dealing with for 18 to 36 months minimum until there is an effective vaccine or treatment. We have the time to think through these questions and to think through them rigorously. And our governments have shown, despite what citizens have often thought, that government really can move pretty quickly when it needs to. And so some of these conversations, and some of these things require a little bit more thinking. Yeah, they totally do. But our governments have actually shown a surprising engagement on these issues. This isn't all government attention. We have the federal bureaucrats that are willing to spend the time. We have the security community, who is very willing to spend the time, we have the legal community who's spending the time, everyone is involved. This is a whole society effort. So that means I think, you know, if it takes us an extra week to figure some of these questions out, or a month, is that a shame? Absolutely. But if we don't get it, right, the harms that we could unleash, not just to the app, a few secondary implications, are pretty profound. And I think we want to defray those risks before we start deploying these solutions to the current pandemic.

Lena Trudeau
I love that, Chris, because you raised that issue of seniors and the fresh hell of the groups that would prey on them and do today and this new avenue. So as with some other things in COVID, if we also give some priority and attention, even based on that issue, because of COVID, and it has the net effect of solving some of those systemic issues, then we're seeing it elsewhere, right, we're seeing it in will everyone really have to return to work? What about virtual care and the progress that we've been able to make, we didn't necessarily ask for it in this form, but some of these things are working. So I think there's also that creative thinking and wearing the risk lens at the same time in terms of addressing some of these very important issues around the communities where we might well see new nefarious approaches. So I'm really glad that you raised that one as well.

Brendan Dowling
The final comment I'd make on the security aspects, I guess is there's some sort of silver lining here. When you look at you know, the speed at which malicious actors take advantage, you know, the phishing campaigns, looking to capitalize on the COVID, say, back in Australia, you know, the speed at which they are deployed is extraordinary. Within 24 hours, people are getting text messages with malicious links. I think the effort at education around that, the fact that everyone is living far more of a professional and personal lives online. Perhaps one opportunity that this period does present is a broad society lift in our cyber security measures, you know, we all know that most of the vulnerabilities, the most common vulnerabilities are because none of us are very good at cybersecurity governments aren't businesses aren't a lot of the basic stuff we can do to protect ourselves. Most people aren't doing. Do we see this as a time where people are much more mindful of those issues, maybe are exposed to a bit more education, maybe make more of an effort on those sort of basic cyber security measures? Can government actually capitalize on that and put out better material, more clearer

material to help people go through that and do we do we see some of those adherence to basic cybersecurity principles improved through this period? You know, I'd hope so and perhaps we will. So I think it there's an opportunity here for governments for industry, for the community for us to open to our grandparents, you know, there's an opportunity for everyone to to use this time to kind of leave those standards.

Lena Trudeau
Thank you all. James, did you have any final thoughts you wanted to share?

James Petrie
In terms of security and for contact tracing? We've talked a lot about privacy. There's also the security of how these alerts are sent out. So I think our model and number of other teams models to require like codes from public health authorities, but I think we should be aware of ways that that can be like, worked around or like to make sure that people can't falsely send out reports to thousands of people to quarantine or things like that. And just to make sure we're not missing something there.

Lena Trudeau
Thank you for that. And Sylvie, we have again saved the best for last.

Sylvie Frigon
Big shoes to fill after all of this. Um, I think the only thing that comes to mind is, from a technology perspective. There's a lot of promises with technology. But we can't put all the eggs in one basket. And I think we've had a bit of a side conversation about, and I think it was, Brendan mentioned that people might become confidence in the technology, and forget about the human aspect. And one thing that popped to my mind is what's what's what tools are in place, if you have an app that works really, really well. But when people receive notification that you might have been exposed to it on what to do. So all of that has to be really again, contextualize into a wider this discussion about all the tools that are needed. And I don't think that technology again is going to resolve all of the issues that we have, but it's also a tool that's very much worth I think exploring and getting ready for now and for the next few months, the next few years and hopefully not the next pandemic, but the next time that we need this kind of wider communication. So lots of work to be done.

Lena Trudeau
Lots of work to be done. Absolutely true. And thank you for the reminder, from everyone that this, as usual, isn't really about the technology or even the security protocols, although we have work to do on that front as well. And James, your point, made a couple of different ways. It's very well taken that we can't afford to get this wrong. And we have to be thoughtful about the way that we deploy the technology and the security protocols. But there's a legal context to this. There is a social context to this. There's a behavioral piece, it comes down to people and their understanding of what they're being asked to do, and what the trade offs are that that we're discussing with the people who will be most affected. And so, as usual, it's about ensuring that those communities are at the table, that we're taking all perspectives into account and that we're not allowing ourselves to think that we have to do something right this very second, if we haven't given sufficient thought to those other elements,

because there are, there are other risks inherent in moving too quickly, without the right kind of preparation and thoughts. So thank you. Thank you for all of this.

Lena Trudeau
Jeremy, I'm going to turn it back over to you to close this out here. And I just want to thank everybody on the panel for doing a fabulous job as, as I can tell you from being in the pre discussion with these folks, I learned an enormous amount and the the research the great experience and context from dealing with these issues over the course of many years, and then the pragmatic view of what it's really looking like to deploy these technologies out in the world has been a great, a great integration of perspectives, and I found it very valuable. So thank you all for everything you've contributed. Jeremy.

Jeremy Dapow
Yes. Just to reinforce that, you know, thank you all for your dedication to the subject, the research that you're doing and, and all of the important contributions that you're making to both the discussion and and figuring out both how to use technology to contain COVID-19 and other pandemics or other diseases, but also keep mindful of all the other considerations, including safety and privacy. So Franca, I want to thank Franca very much for all her work in supporting this, and the Internet Society, Canada chapter. Lena, thank you for your leadership and moderating. I also want to thank the US Embassy in Canada and Amazon Web Services for their funding partnership. As well as all the other organizations that we're working with and are our friends and allies and Australia High Commission and UK High Commission, and we greatly appreciate that, that collaboration and that what makes us very meaningful. So, then lastly, our steering committee for helping to determine what, what we should engage in and also helping us to do it. Right. So we really do hope you enjoyed this session. And it's been recorded and it will be uploaded. And we're going to do a little summary for folks and, again, thank you very much for participating and, and we hope we you have a wonderful rest of your day, and stay safe and stay healthy. Thank you.

Lena Trudeau
Thanks, everyone.

Franca Palazzo
Thank you, everyone.